Inhalt

Vierter Teil
Sondervoten der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN

A. Gemeinsames Sondervotum der Fraktionen DIE LINKE. und BÜNDNIS 90/DIE GRÜNEN

I. Zusammenfassung

1. Blockadehaltung der Bundesregierung mit Unterstützung der Mehrheit

Aus Perspektive der Oppositionsfraktionen war der 1. Untersuchungsausschuss der 18. Wahlperiode wichtig und ausgesprochen erfolgreich. Trotz der kritikwürdigen Blockadehaltung der Bundesregierung und ihres aktiven Hintertreibens der parlamentarischen Aufklärung, ist es uns gelungen, die durch Edward Snowden bekannt gewordenen, rechtsstaatlich problematisch bis offen rechtswidrigen Geheimdienstpraktiken weiter aufzuklären und eine ganze Reihe von zusätzlichen Problemfeldern, Informationen und skandalösen Verfehlungen an die Öffentlichkeit zu bringen.

Wesentlich erschwert und faktisch behindert wurde die Aufklärung durch eine Bundesregierung, die keinerlei Interesse zeigte, klar untersuchungsgegenständliche, offenkundig rechtlich problematische Praktiken und Kooperationen deutscher Geheimdienste zu offenbaren, geschweige denn sie aufzuarbeiten und zu korrigieren. Viele Geheim-Einstufungen von Akten und Vorgängen lassen sich nur durch den Grad der politischen Peinlichkeit erklären, die ein Bekanntwerden des eingestuften Vorgangs der Bundesregierung verursacht hätte.

Das Grundgesetz selbst enthält mit Art. 44 das Recht des Parlaments, einen Untersuchungsausschuss einzusetzen und legt das Grundprinzip der Öffentlichkeit der Untersuchung fest. Die Bundesregierung jedoch hat von Anfang an und umfangreichst Akten geschwärzt bzw. aus den Übersendungen pauschal heraus genommen, den Ausschuss gleichzeitig in schlecht aufbereiteten Aktenmassen schier ertränkt, Einstufungen von Akten und Sitzungen vorgegeben, denen die Ausschussmehrheit von CDU/CSU und SPD dann oftmals als „Schutztruppe der Regierung" (*Brocker*, DÖV 2014) gehorsam gefolgt ist, und beständig neue Verfahren erfunden, mit denen die Akteneinsicht auf verschiedene Orte außerhalb des Bundestages verlegt wurde. Es

hat eine Unzahl „streng geheim“ eingestufter Ausschusssitzungen gegeben, obwohl oftmals nicht zu erkennen war, wie durch das öffentlich werden des Inhaltes der Sitzung das Fortbestehen der Bundesrepublik jemals in Gefahr hätte geraten können. Den Ausschussmitgliedern wurde mehrfach pauschal unterstellt, Geheimnisse zu verraten. Es wurde ihnen mit strafrechtlichen Ermittlungen gedroht. Dabei beschworen Vertreter_innen der Exekutive öffentlich die Gefahr von aus der parlamentarischen Untersuchungsausschussarbeit resultierenden Terroranschlägen, die die Folge davon wären, dass sich die Partner der deutschen Geheimdienste aus den Kooperationen zurückzögen, weil das Parlament seinem Auftrag nachkam, jahrelanges rechtswidriges Verhalten eben dieser Dienste zu untersuchen.

2. Keine Zeugenaussage von *Edward Snowden*

Durch die couragierten Enthüllungen von *Edward Snowden* hat die Welt erfahren, dass die Geheimdienste der Five Eyes die Digitalisierung dazu nutzen, ein invasives System der totalen Überwachung voranzutreiben. Snowden wurde als erster Zeuge des Untersuchungsausschusses benannt; seine Aussage wäre für den Ausschuss von größter Bedeutung gewesen. Dass es uns nicht gelungen ist, diese Aussage zu ermöglichen, liegt an den konzertierten Bemühungen der Bundesregierung und der Ausschussmehrheit der Großen Koalition und wurde von Gerichtsentscheidungen gestützt, die wir bedauern.

Das enthebt uns nicht der Verantwortung, uns weiter dafür einzusetzen, Edward Snowden ein Leben frei von politischem Druck zu ermöglichen und darauf zu hoffen, dass er dem Bundestag in der Zukunft Einblick in seine Erkenntnisse über die Massenüberwachung in Deutschland doch noch geben kann.

3. Massenüberwachung in Deutschland und international

Anlasslose und unzulässige Massenüberwachung hat die Beweisaufnahme nicht nur im Rahmen der Operation EIKONAL festgestellt, sondern auch darüber hinaus mittels NSA- und BND-Selektoren. Auch deutsche Staatsbürger_innen und Unternehmen waren davon über Jahre betroffen. Direkte Massenüberwachung durch die NSA in Deutschland und darüber hinaus im Ausland von Deutschland aus konnte nicht näher

aufgeklärt werden, weil Akten und Zeugen aus Großbritannien und den USA nicht zur Verfügung standen.

Der Begriff „Anlasslose Massenüberwachung“ wurde als Folge der Snowden-Enthüllungen geprägt. Er bringt die besondere Qualität der seit 2013 bekanntgewordenen Überwachungsinfrastruktur zum Ausdruck. Viele Einzelheiten der in den Dokumenten veröffentlichten Systeme und Aktivitäten der Five Eyes konnten im Ausschuss nicht untersucht werden, weil die Bundesregierung dem Ausschuss fast alle Akten mit Bezug zu den Geheimdiensten der USA, Großbritanniens, Kanadas, Australiens und Neuseelands pauschal vorenthielt. Es gab aber auch keinerlei Anlass und keine Zeugenaussage, die Grund böten, am Wahrheitsgehalt der Snowden-Dokumente zu zweifeln. Dass insbesondere der BND Teil dieser weltweiten Überwachungsstruktur ist, wurde im Ausschuss eindrucksvoll belegt.

4. Die Kooperation des BND mit der NSA in Bad Aibling

Das Memorandum of Agreement, eine Vereinbarung von 2002 zwischen BND und NSA über gemeinsame Telekommunikationsüberwachung in Deutschland sollte der NSA auch Zugriff auf Daten am Frankfurter Netzknoten verschaffen, war jedoch mangels nötiger Zustimmung des Bundestages formell unwirksam.

5. Datenabgriffe in Frankfurt ohne G 10-Anordnung

Zwischen 2005 und 2008 fanden in Frankfurt/Main im Rahmen der gemeinsamen Operation EIKONAL des BND mit der NSA Datenabgriffe durch den BND ohne Rechtsgrundlage statt. Entgegen massiver Bedenken der eigenen Mitarbeiter_innen wurde die Operation [redacted], ohne dass es dafür G 10-Anordnungen gab. Dabei wurden Daten in Deutschland an den BND ausgeleitet und das Fernmeldegeheimnis über Jahre unbefugt gebrochen. [redacted] der BND haben so bewusst die existierenden parlamentarischen Kontrollregime über Jahre getäuscht und unterlaufen sowie einen andauernden Rechtsbruch billigend in Kauf genommen.

6. Der Mythos der funktionierenden Filter

Die praktische Umsetzung der Operation EIKONAL steht beispielhaft für den Ansatz der NSA, Überwachungsmaßnahmen gemeinsam mit den jeweiligen Geheimdiensten vor Ort durchzuführen. Dabei war das Ziel durch das Tauschgeschäft „Daten gegen Technik" die Überwachungsmaßnahmen technisch entscheidend mitzugestalten: Die NSA liefert Hard- und Software, BND und BfV Daten und Informationen.

Die für die Kabelerfassung erforderliche Technik hätte hier vom BND schon deswegen nicht eingesetzt dürfen, weil sie ohne vollständige Prüfung durch das BSI „zertifiziert" wurde. Die eingesetzten Datenfilter waren nie in der Lage, die G 10-geschützte Kommunikation vor der Weiterleitung an die NSA zuverlässig auszufiltern.

7. Problematische Selektoren der NSA in den Daten des BND

Teil der Kooperation zwischen BND und NSA war und ist, dass der BND die von ihm erfassten Daten mithilfe von Suchbegriffen der NSA filtert. Die Ergebnisse werden dann an die NSA weitergeleitet. Auf dem Papier hätten alle Kommunikationsdaten, die Deutsche betreffen, ausgefiltert werden sollen. Obwohl die Akten zu diesen Selektoren dem Ausschuss sofort hätten übergeben werden müssen, weil dies zentrale Fragen des Untersuchungsauftrags berührt, bedurfte es eines eigenen Beweisantrags der Opposition. Sehr viele Selektoren betrafen weder Terrorismus noch illegalen Waffenhandel, sondern berührten deutsche und europäische Interessen. Letztlich konnte dieser Komplex aber nicht aufgeklärt werden, weil die Bundesregierung dem Ausschuss die Einsicht in die NSA-Selektoren verweigerte. Über das frei erfundene Konstrukt der „Vertrauensperson der Bundesregierung", die gemeinsam mit dem BND die NSA-Selektoren untersuchte, wurde eine Aufklärung vorgegaukelt, die real nie stattfand.

8. Datenübermittlung des BND an die NSA aus Bad Aibling

Im Rahmen der Kooperation in Bad Aibling übermittelte der BND monatlich rund 1,3 Mrd. Daten an die NSA. Der BND unterschied dabei unzulässig zwischen Inhalts- und Metadaten, obwohl auch Metadaten geeignet sind, intimstes Wissen über Betroffene preiszugeben. Metadaten wurden massenhaft erfasst und verarbeitet, die Rohdatenströme ganzer Kommunikationsstrecken automatisiert an die NSA weitergeleitet.

Diese automatisierte und unterschiedslose Weiterleitung aller erfassten Metadaten ist unverhältnismäßig und offenkundig rechtswidrig.

9. Die Operationen GLO[redacted] und M[redacted]S[redacted]

Neben der Operation EIKONAL hat sich der Untersuchungsausschuss mit GLO[redacted] einer weiteren Operation des BND gemeinsam mit einem US-amerikanischen Geheimdienst sowie der Operation M[redacted]S[redacted], einem Projekt zur Kabelüberwachung mit einem britischen Geheimdienst befasst. Die Untersuchung beider Operationen war nur sehr eingeschränkt möglich. Die Ergebnisse zeigen aber, dass der BND auch hier vorsätzlich an den Kontrollgremien vorbeigearbeitet hat. Während das deutsch-britische Projekt unmittelbar nach den Snowden-Veröffentlichungen gestoppt wurde, wurde die Operation GLO[redacted] unter Vorspiegelung falscher Tatsachen durchgeführt. Dabei wurden rechtswidrig Kommunikationsdaten erfasst und verarbeitet.

10. Die Selektoren des BND

Nicht nur die NSA sucht nach Informationen in den erfassten Daten, der BND setzt auch eigene Selektoren ein. Durch die Erweiterung des Untersuchungsauftrags wurde deutlich, dass auch diese Selektoren nicht nur die Bereiche des Auftragsprofils des BND betrafen, sondern etwa befreundete Regierungen, europäische Institutionen, internationale Organisationen, Journalist_innen und die Zivilgesellschaft. Eine öffentliche Untersuchung des Themas wurde von der Bundesregierung verhindert. Die Bundeskanzlerin war nach eigenem Bekunden selbst ahnungslos bzgl. des Agierens des eigenen Geheimdienstes, als sie sich empört zur Überwachung ihres eigenen Handys äußerte und erklärte „Abhören unter Freunden – das geht gar nicht“.

11. No-Spy-Abkommen, die Wahlkampflüge des Herrn *Pofalla*

Mit der Behauptung, die US-Seite habe angeboten, „uns nicht auszuspionieren“, zog die damalige Bundesregierung fünf Wochen vor der Bundestagswahl 2013 die Notbremse, um das äußerst ärgerliche und lästige Thema des Sommers einer unzulässigen und rechtswidrigen, anlasslosen und massenhaften Ausspähung von Millionen

durch NSA und BND zu beerdigen. Diese Erklärung war falsch. Es gab lediglich Vorschläge für eine Arbeitsgruppe zu Gesprächen über nachrichtendienstliche Probleme, aber kein „Angebot“ für ein „No-Spy-Abkommen“. Ganz im Gegenteil legte das Weiße Haus wert auf die Feststellung, dass von US-Seite von Anfang an und fortwährend klar gemacht wurde, ein solches Abkommen werde nicht geben. Aber da war die Wahl gelaufen und der Zweck der Erklärung *Pofallas* erreicht.

12. Der blinde Fleck der Wirtschaftsspionage

Die Spionageabwehr ist Aufgabe des BfV. Trotz zahlreicher Hinweise auf (Wirtschafts-)Spionage durch Geheimdienste sogenannter befreundeter Staaten, verharrt das BfV in den Denkmustern des Kalten Krieges. Gezielte Spionageabwehr findet – wenn überhaupt im Digitalen – gegenüber Staaten wie Russland und China statt, bei befreundeten Staaten, wie denen der Five-Eyes wird offenkundig weggesehen trotz proklamiertem „360°-Blick“. Dabei krankt die Spionageabwehr auch an der Tatsache, dass mit dem BND ein Geheimdienst des Bundes einen willfährigen Dienstleister der NSA gibt, anstatt das BfV auf Erkenntnisse hinzuweisen.

13. Die Hauptstelle für Befragungswesen: Freiwillige Informationen für den Drohnenkrieg?

Unter der Legende „Hauptstelle für Befragungswesen“ betrieb der BND bis Sommer 2014 eine Tarnbehörde, die in Kooperation mit US-amerikanischen und britischen Nachrichtendiensten vor allem Asylbewerber_innen ausfragte. Dass sie – teils allein – von US-Geheimdienstmitarbeiter_innen befragt wurden, wussten diese nicht. Es gab weder eine Rechtsgrundlage für die Befragungen selbst, noch für die Übermittlung der Daten an die USA. Fragwürdig ist auch die enge Zusammenarbeit der HBW mit dem Bundesamt für Migration und Flüchtlinge, das dem BND erst die nötigen Hinweise auf möglicherweise interessante Personen gab. Die HBW wurde im Sommer 2014 formal aufgelöst. Befragungen von Asylbewerber_innen durch deutsche Nachrichtendienste finden gleichwohl bis heute statt.

14. Der Geheime Krieg und die Rolle der US-Basis in Ramstein: Die Bundesregierung trägt Verantwortung für die Drohnentoten

Die Rolle Deutschlands im US-Drohnenkrieg ist klar: Die US-Luftwaffenbasis Ramstein ist der zentrale Drehpunkt des US-Drohnenprogrammes in Europa. Hier laufen nicht nur die Daten zwingend zusammen, die nötig sind, damit die Drohnen fliegen können. Das hat die Beweisaufnahme und insbesondere die Aussage des Zeugen *Brandon Bryant*, einem ehemaligen US-Drohnenpiloten, deutlich gemacht. Ebenfalls steht fest, dass die Bundesregierung seit vielen Jahren die Augen vor der Bedeutung Ramsteins für das US-Drohnenprogramm verschließt. Schon 2011 hatte sie Kenntnis davon, dass Entscheidungen für gezielte Tötungen in Ländern wie dem Jemen, Somalia oder Pakistan und damit der Tod hunderter ziviler Opfer auch auf deutschem Boden mitverantwortet werden. Relevantes dagegen getan hat sie nicht. Die Bundesregierung steht rechtlich in der Verantwortung und hat ihre Pflichten zur Herstellung von grund- und völkerrechtsmäßigem Verhaltens der US-Streitkräfte auf deutschem Boden bislang nur unzulänglich wahrgenommen. Stattdessen hat sie jahrelang den deutschen Bundestag bei der Beantwortung direkter parlamentarischer Fragen zu diesem Thema über die Sach- und eigene Erkenntnislage getäuscht.

II. Einleitung

1. Die Folgen der Snowden-Enthüllungen

Am 6. Juni 2013 erschien der erste Artikel, der auf den Enthüllungen von *Edward Snowden* basierte. Ein Datum, das eine Zeitenwende markiert, mit der für viele Nutzerinnen und Nutzer zum ersten Mal spürbar wurde, dass die Zeit des ‚freien Internets' beendet und Orwells Dystopie der totalen Überwachung eine reale Option war. Umgesetzt auch von Geheimdiensten der westlichen Welt – deren Aufgabe eigentlich der Schutz von Demokratie und Meinungsfreiheit sein sollte.

Schnell wurden Fragen laut, ob die Geheimdienste der USA und Großbritanniens, NSA und GCHQ, in Europa und damit auch in Deutschland genauso skrupellos Daten sammeln, speichern und auswerten. Was wusste die Bundesregierung darüber? Waren die deutschen Nachrichtendienste BND, Verfassungsschutz und MAD ahnungslos, oder hatten sie ihr Wissen für sich behalten?

Nach dem ersten Schock mitten im Bundestagswahlkampf hatte sich die damalige schwarz-gelbe Bundesregierung entschieden, das Problem möglichst unter den Teppich zu kehren. Am 12. August stand Kanzleramtsminister *Ronald Pofalla* vor den Kameras und erklärte die NSA-Affäre für beendet. Da waren viele Artikel noch gar nicht veröffentlicht, die auf den Snowden-Dokumenten basierten.

2. Einsetzung des Untersuchungsausschusses

Die SPD, noch Opposition, protestierte und forderte umfassende Aufklärung. Als im Oktober bekannt wurde, dass die NSA selbst vor dem Handy der Kanzlerin nicht Halt machte, wurde deutlich, dass das Thema per Dekret nicht zu beenden war. Bereits in der 2. Sitzung des neugewählten Bundestages wurde über die Abhöraktivitäten der NSA und die Auswirkungen auf Deutschland und die translatlantischen Beziehungen debattiert[1]. Grundlage waren Entschließungsanträge der Fraktionen DIE LINKE.[2] und

1) Plenarprotokoll 18/2

2) Bundestagsdrucksache 18/56

BÜNDNIS 90/DIE GRÜNEN[3]. In dieser Debatte wurde nicht nur über die Notwendigkeit eines Untersuchungsausschusses gesprochen, sondern – von Politikern der Opposition – auch darüber, wie und wo *Edward Snowden* vom Parlament befragt werden könnte.

Nach langwierigen Verhandlungen darüber, was untersucht werden sollte, wurde der 1. Untersuchungsausschuss eingesetzt, der oft NSA-Untersuchungsausschuss genannt wurde, später aber genauso gut BND-Untersuchungsausschuss hätte heißen können – nicht zuletzt, weil eine wirksame Untersuchung der NSA-Aktivitäten von der Großen Koalition verhindert wurde.

Thema der Untersuchung sollte die Massenüberwachung der Five Eyes in Deutschland sein, aber genauso auch, was die Bundesregierung davon wusste und welche Rolle deutsche Dienste dabei spielten. Ein wichtiges Kapitel sollte auch die mögliche Beteiligung Deutschlands am Drohnenkrieg der USA sein: Über die Duldung der Relaisstation auf der US-Militärbasis in Ramstein, die mögliche Weitergabe von Daten, die für die Zielfindung der Drohnen genutzt werden können und die Befragung von Geflüchteten in Deutschland durch die Geheimdienste.

3. Proteste gegen Massenüberwachung

Der Untersuchungsausschuss ist nicht allein das Ergebnis der Arbeit im Parlament. Die zahlreichen Aktivitäten und Proteste gegen Überwachung seit dem Sommer 2013 haben wesentlich dazu beigetragen, dass der Ausschuss zustande kam.

Tausende Menschen demonstrierten im Juli in vielen deutschen Städten im Rahmen des Bündnisses *Stop Watching Us* und im August beim *International Day of Privacy*. Es gab Spaziergänge vor dem Gebäude des BND in Berlin, zur BND-Außenstelle in Schöningen und am Dagger-Komplex in Griesheim[4]. Im Rahmen der Aktion „Ein Bett für Snowden“ forderten 40 000 Menschen Asyl für *Edward Snowden* in Deutschland.[5]

3) Bundestagsdrucksache 18/65

4) *Spiegel Online* vom 15. Juli 2013 „Spaziergang ruft Staatsschutz auf den Plan“, abrufbar unter http://www.spiegel.de/netzwelt/netzpolitik/spaziergang-zum-dagger-complex-interessiert-die-polizei-a-911215.html

5) *Campact*: Ein Bett für Snowden, abrufbar unter https://www.campact.de/snowden/ein-bett-fuer-snowden/

Über sechzig Schriftstellerinnen und Schriftsteller forderten in einem Offenen Brief an die Kanzlerin Aufklärung.[6] Er wurde von 80 000 Menschen mitunterzeichnet.[7] Viele Menschen haben sich zum ersten Mal damit beschäftigt, wie sie sich selbst vor Überwachung schützen und beispielsweise ihre Kommunikation verschlüsseln können.

All dies hat uns erreicht und uns darin bestärkt, uns für die Aufklärung im Parlament einzusetzen.

4. Die Arbeit des Ausschusses war wichtig

Der Untersuchungsausschuss hat in gut drei Jahren viel erreicht. Wir wissen heute mehr über die Arbeit der Geheimdienste in Deutschland, und dabei vor allem über den Bereich der technischen Aufklärung. Trotz vieler Versuche der Bundesregierung und der Regierungsfraktionen, die Aufklärung an vielen Punkten stark zu beschränken, fällt unser Fazit nach knapp drei Jahren positiv aus. Neben einer Untersuchung im Europäischen Parlament[8] und einem Ausschuss in Brasilien war dieser Untersuchungsausschuss international der einzige, der von einem Parlament zur Untersuchung der von Snowden enthüllten Informationen eingesetzt wurde.

5. Der Schutz der Privatsphäre ist ein universelles Recht

Viele der Ergebnisse der Untersuchung befassen sich mit der Verletzung von Grundrechten, also Rechten, die das Grundgesetz garantiert. Zentral berührt wurde der Schutz des Brief-, Post- und Fernmeldegeheimnisses nach Artikel 10 des Grundgesetzes.

Es ist uns wichtig zu betonen, dass wir uns nicht deshalb vorrangig mit den Rechten der Bevölkerung in Deutschland befasst haben, weil sie uns wichtiger wären als die

---

6) *FAZ Online* vom 25. Juli 2013 „Deutschland ist ein Überwachungsstaat“, abrufbar unter http://www.faz.net/aktuell/feuilleton/debatten/ueberwachung/offener-brief-an-angela-merkel-deutschland-ist-ein-ueberwachungsstaat-12304732.html

7) *Change.org*: Angemessene Reaktion auf die NSA-Affäre – Petition von Juli Zeh, abrufbar unter https://www.change.org/nsa

8) LIBE Committee Inquiry on Electronic Mass Surveillance of EU Citizens
http://www.europarl.europa.eu/committees/de/libe/subject-files.html?id=20130923CDT71796, abgerufen am 22. Mai 2017

Menschen in allen anderen Ländern. Unsere Aufgabe war es zu prüfen, ob und wie sich die Bundesregierung und ihre Behörden rechtswidrig verhalten haben. Auch wenn wir der Meinung sind, dass die Kommunikation aller Menschen gleichermaßen dem Schutz des Artikel 10 unterfallen sollte, sieht die Bundesregierung dies dezidiert anders – entgegen übrigens der Meinung führender Verfassungsrechtler_innen. Die deutschen Geheimdienste sind demnach verpflichtet, bei der Überwachung von Deutschen mehr Vorsicht walten zu lassen als bei der Überwachung im Ausland. Daran haben wir sie gemessen.

Bei der Untersuchung der Aktivitäten des BND im Ausland waren uns enge Grenzen gesetzt. Für eine Aufklärung der digitalen Überwachung weltweit bleibt noch viel zu tun. Wir sind aber überzeugt, dass uns mit der Arbeit dieses Untersuchungsausschusses gelungen ist, einen wichtigen Baustein beizutragen.

III. Bewertungen und Anmerkungen zum Verfahren

Vor der Bewertung der Ergebnisse im Detail ist es notwendig, auf die Rahmenbedingungen der Arbeit des NSA-Untersuchungsausschusses einzugehen.

Die Ausschussmehrheit zeichnet in ihrem Bericht das Bild einer mit dem Ausschuss beinahe vorbildlich kooperierenden Bundesregierung und einer deshalb angemessenen Aufklärungsarbeit des Ausschusses. So liegt es jedoch nicht. Vielmehr hat die Bundesregierung in Kooperation mit einer überdeutlich als „Schutztruppe der Regierung“[9] agierenden Ausschussmehrheit die Aufklärungsarbeit des Ausschusses in unerträglicher Weise und über das „normale“ Maß hinausgehend erschwert und behindert.

Die Arbeit des Untersuchungsausschusses war in den vergangenen drei Jahren beständig den Versuchen der Bundesregierung ausgesetzt, die Aufklärung faktisch zu behindern. Unterstützt wurde sie dabei von den Vertreter_innen der Großen Koalition im Ausschuss, die der Presse gegenüber ihr Aufklärungsinteresse zwar regelmäßig betont haben, de facto hinter verschlossenen Türen aber das Gegenteil getan haben. Die Auseinandersetzung um die – letztlich von CDU/CSU und SPD verhinderte – Ladung von Edward Snowden als Zeuge in den durch ihn erst ermöglichten Ausschuss ist hierfür das beste Beispiel.

Auch unter rechtsstaatlichen Gesichtspunkten ist dabei besonders beunruhigend, dass die Gegenseite noch nicht einmal davor zurückschreckte, den Zeugen auf eine Weise zu diskreditieren, die sich in der Nähe eines strafbaren Handelns bewegte. So stellten sowohl der Ausschussvorsitzende Sensburg als auch der Präsident des Bundesverfassungsschutzes Maaßen die Behauptung in den Raum, Herr Snowden sei Agent der Russen; eine Tatsachenbehauptung für die der Nachweis, dass diese Tatsache „erweislich wahr“ (§ 186 StGB) ist, selbstverständlich nicht zu führen war und ist, wie auch die Ausschussmehrheit zugibt.

---

9) *Brocker*: Die „Splitterenquete“: Rechte der nicht qualifizierten („einfachen“) Minderheit im parlamentarischen Untersuchungsverfahren, DÖV 2014, S. 475

Wenn es nicht gelungen ist, die Aktivitäten der Geheimdienste der Five Eyes in Deutschland zu beleuchten, dann liegt dies zum einen an der Verweigerung der Regierungen der beteiligten Staaten USA, Großbritannien, Kanada, Australien und Neuseeland, und zum anderen an der Bundesregierung, die sich unter Missachtung der Grundprinzipien parlamentarischer Kontrolle weigerte, dem Bundestag relevante Dokumente zu übergeben und Aussagegenehmigungen im gebotenen Umfang zu erteilen.

Ganz besonders schmerzlich war, dass der Ausschuss keinen Zugang zu den von den deutschen Geheimdiensten eingesetzten Selektoren der NSA erhielt. Die Arbeit deutscher Geheimdienste konnte daher in diesem Bereich allenfalls eingeschränkt aufgeklärt werden.

In nie gekanntem Umfang wurden Akten geschwärzt, dem Ausschuss vorenthalten, fehlerhaft als geheimhaltungsbedürftig eingestuft und im Übrigen der Zugang zu Akten dadurch erschwert, dass den Abgeordneten der Zugriff nur außerhalb des Bundestages gestattet wurde. Diese Vorgänge waren dabei so zahlreich, dass von vorneherein – auch angesichts begrenzter Ressourcen der Oppositionsfraktionen – ausgeschlossen war, über jeden dieser Vorgänge eine Einzeldiskussion mit der Gegenseite zu führen. Die Politik der Gegenseite war hier darauf angelegt, die Arbeit der Oppositionsfraktionen im Ausschuss auch durch die reine Masse der Streitfragen zu erschweren.

1. Erschwerung der Aufklärung durch die Mehrheit

a) Berliner Stunde

Die Arbeit im Ausschuss wurde erheblich erschwert, weil die Mehrheit darauf beharrte, bei Zeugenbefragungen an der in der sogenannten ‚Berliner Stunde' definierten Redezeitverteilung festzuhalten. Danach standen, in dieser Reihenfolge, pro Stunde 27 Minuten der CDU/CSU-Fraktion, acht Minuten der Fraktion DIE LINKE., 17 Minuten der SPD-Fraktion und schließlich acht Minuten der Fraktion Bündnis 90/Die Grünen zu. Der Vorsitzende kann zudem ohne jede zeitliche Begrenzung fragen. Zwar war die

Zahl der Frage-Runden nicht begrenzt, so dass im Lauf der Vernehmung die Fraktionen der Großen Koalition häufig auf ihre Fragezeit verzichteten. Die Auswirkung auf die Zeugenbefragung allerdings war verheerend: Es waren nur selten zusammenhängende Befragungen möglich, weil mit jedem Wechsel zwischen den Fraktionen auch das Thema wechselte. Das ist sowohl für die Zeug_innen belastend als auch für den gesamten Ausschuss, weil es unweigerlich zu zahlreichen Wiederholungen kommt. Die häufig lange Dauer der Vernehmungen, teils bis spät in die Nacht, hat auch hier ihren Ursprung.

Die Zeug_innen haben es so in der Hand Fragen auszuweichen, indem sie für die Beantwortung einer Frage die gesamte Fragezeit der fragenden Fraktion ausschöpfen: Denn die Beantwortung einer Frage wird auf die Fragezeit angerechnet.

b) Verzögerung der Erweiterung des Untersuchungsauftrags

Mit der Untersuchung der NSA-Selektoren gab es Anlass zur Vermutung, dass der BND selbst ebenfalls Selektoren einsetzte, die gegen deutsche und europäische Interessen verstießen. Bereits im Sommer 2013 hatte die Bundeskanzlerin zum ersten Mal während der Sommerpressekonferenz kategorisch erklärt, dass sich ihrer Ansicht nach gegenseitige Spionage unter Partnern verbiete:

> „Um jetzt noch einmal klar etwas dazu zu sagen, was wir über angebliche Überwachungen auch von EU-Einrichtungen usw. gehört haben: Das fällt in die Kategorie dessen, dass man das unter Freunden nicht macht. Das geht nicht.“[10]

Als im Herbst 2013 bekannt wurde, dass auch ihr eigenes Handy von der NSA überwacht wurde, wiederholte sie:

> „Ausspähen unter Freunden: Das geht gar nicht“[11]

---

10) Sommerpressekonferenz von Bundeskanzlerin *Merkel* vom 19. Juli 2013, Skript abrufbar unter https://www.bundesregierung.de/ContentArchiv/DE/Archiv17/Mitschrift/Pressekonferenzen/2013/07/2013-07-19-merkel-bpk.html

11) *Spiegel TV* vom 24. Oktober 2013 „Merkel empört über Handy-Affäre. „Das geht gar nicht!“, abrufbar unter http://www.spiegel.de/video/merkel-empoert-ueber-handy-affaere-das-geht-gar-nicht-video-1304485.html

Umso mehr war es erforderlich, im Rahmen des Untersuchungsausschusses nicht nur problematische NSA-Selektoren zu untersuchen, sondern auch die möglicherweise ähnliche Praxis des BND zu beleuchten. Dies wurde jedoch zunächst mit dem Hinweis verunmöglicht, dies sei eben nicht Bestandteil des Untersuchungsgegenstands.

Die Opposition hat am 17. Februar 2016 einen Antrag zur Erweiterung des Untersuchungsauftrags vorgelegt.[12] Die Verhandlungen mit der Mehrheit zogen sich über dreieinhalb Monate, bis die Erweiterung schließlich in erheblich reduzierter Form am 9. Juni 2016 im Bundestag verabschiedet wurde.[13]

2. Behinderung des Ausschusses durch die Bundesregierung

a) Aktenvorlage

Grundlage für die Befassung des Untersuchungsausschusses mit den verschiedenen im Untersuchungsauftrag benannten Themen sind Unterlagen der verschiedenen Ministerien und Behörden der Bundesregierung. Der Ausschuss fasst Beweisbeschlüsse, in denen konkret benannt wird, welche Akten vorzulegen sind und die Regierung ist verpflichtet, alle einschlägigen Akten zu identifizieren und dem Untersuchungsausschuss zu übergeben. Nur bei Vorliegen der in der Verschlusssachenanordnung (VSA) geregelten Voraussetzungen dürfen die Unterlagen von der Bundesregierung mit einem Geheimehlatungsgrad versehen und entsprechend gekennzeichnet werden.

Falls nötig, werden solche Akten, die den verschiedenen Stufen der Geheimhaltung unterliegen (oder: „eingestuft“ sind), durch die Geheimschutzstelle des Bundestages entspechend gekennzeichnet. Solche als „vertraulich“, „geheim“ oder „streng geheim“ eingestuften Akten dürfen nur von sicherheitsüberprüften Mitarbeiter_innen gelesen werden, und von den Mitgliedern des Bundestages (MdB). Diese Akten, so hat das

12) Ergänzung des Untersuchungsauftrages des 1. Untersuchungsausschusses – Hilfsweise: Einsetzung eines Untersuchungsausschusses, BT-Drucksache 18/7565

13) Beschlussempfehlung und Bericht des Ausschusses für Wahlprüfung, Immunität und Geschäftsordnung (1. Ausschuss) vom 6. Juni 2016, BT-Drucksache 18/8683

Bundesverfassungsgericht in seinem Urteil zu einer Klage der Opposition im so genannten „BND-Untersuchungsausschuss“ des Bundestages vor zwei Wahlperioden entschieden,

> „sind bei der Untersuchung politischer Vorgänge ein besonders wichtiges Beweismittel. Sie haben gegenüber Zeugenaussagen in der Regel einen höheren Beweiswert, weil das Gedächtnis von Zeugen aus mancherlei Hinsicht unergiebig werden kann.“[14]

Tatsächlich gestaltete sich die Aktenvorlage seitens der Bundesregierung als ausgesprochen zäh. Sie war für die gesamte Dauer der Beweisaufnahme Anlass für Auseinandersetzungen zwischen im Wesentlichen der Opposition im Ausschuss und der Bundesregierung.

aa) Unsystematische und unvollständige Schriftgutverwaltung im BND

Nach Sichtung erster Unterlagen, die dem Untersuchungsausschuss auf Grundlage der Beweisbeschlüsse vorgelegt wurden, mussten die Mitglieder der Opposition feststellen, dass es sich bei den zur Verfügung gestellten Ordnern und Kladden keinesfalls um Vorgangs- oder Handakten handelt, sondern Unterlagen aus verschiedenen Geschäftsbereichen des Hauses, die nach nicht nachvollziehbaren Kriterien zum Thema des Vorlagebeschlusses zusammengestellt wurden. Ein verbindlicher Aktenplan im BND wurde weder vorgelegt noch wurde in irgendeiner Form schlüssig erläutert, wie die Aktenführung im BND organisiert ist. Offenbar werden zu einzelnen Sachthemen keine durchgehenden, vollständigen und chronologischen Akten angelegt.

Auch war nicht zu erkennen, dass es Handakten von Beamten in Leitungsfunktion gibt, in denen deren Verwaltungshandeln, aber auch deren Wahrnahme der Rechts-, Fach-, und Dienstaufsicht dokumentiert wird. Aktenwahrheit und -klarheit war ebenso wenig zu erkennen, wie Bemühungen, den minimalsten Anforderungen einer verständlichen und systematischen Aktenführung im Sinne des Datenschutzes und der Rechte behördlicher wie parlamentarischer Kontrollinstanzen gerecht zu werden. Weiterhin

14) BVerfGE 124, 78, zitiert nach http://www.bverfg.de/e/es20090617_2bve000307.html, dort Rn. 113

musste die Minderheit im Untersuchungsausschuss feststellen, dass es zu Vorgängen erheblicher Bedeutung keine Verschriftlichung von Telefonaten noch von Videokonferenzen gab.

Inwieweit digitale Akten zentral als Schriftgut erfasst werden, blieb offen.

b) Interpretation des Untersuchungsgegenstands

Das Bundesverfassungsgericht hat sich in seinem Beschluss im Jahr 2009 sehr klar dazu geäußert, dass sich die Beiziehung von Akten nicht von vornherein auf spezifische klar definierte Tatsachen beziehen müsse:

> „Während im Strafverfahren die Verwirklichung eines bestimmten fest umrissenen Tatbestandes im Hinblick auf die individuelle Schuld einer Person geprüft wird, geht es im Untersuchungsausschuss um die Aufklärung eines Sachverhalts zu politischen Zwecken, vor allem um die Wahrnehmung der Kontrollfunktion des Parlaments. Die einzelne Beweiserhebung eines Untersuchungsausschusses muss dahier nicht auf bestimmte Tatsachen bezogen sein, sondern kann darauf abzielen, zunächst „Licht ins Dunkel“ eines Untersuchungskomplexes zu bringen, um auf diese Weise die Aufklärung von politischen Verantwortlichkeiten zu ermöglichen“.[15]

Und:

> „Bei einem Ersuchen auf Aktenvorlage muss nicht bereits feststehen, dass die Unterlagen auch tatsächlich entscheidungserhebliches Material oder entsprechende Beweismittel enthalten. Es reicht aus, wenn sie Hinweise hierauf geben könnten.“[16]

Dennoch hat die Bundesregierung mit dem lapidaren Hinweis, bestimmte Fragestellungen gehörten nicht zum Untersuchungsgegenstand, wiederholt Akten verweigert,

---

15) BVerfGE 124, 78, zitiert nach http://www.bverfg.de/e/es20090617_2bve000307.html, dort Rn. 111.

16) BVerfGE 124, 78, zitiert nach http://www.bverfg.de/e/es20090617_2bve000307.html, dort Rn. 113.

die konkrete Begründung dazu erst auf Aufforderung nachgeliefert oder auch Akten erst geliefert, nachdem diese mit konkreteren Beweisbeschlüssen angefordert worden waren.

aa) WHARPDRIVE

Im Juni 2014 veröffentlichte *Der Spiegel* die „Deutschland-Akte“, eine Reihe von Artikeln zusammen mit zahlreichen Snowden-Dokumenten mit Bezug zur Bundesrepublik Deutschland. Darin erwähnt wird die Operation WHARPDRIVE, eine

> „Gemeinsame Operation von NSA und BND mit einem dritten Partner, um Zugang zu einer internationalen Datenleitung zu erhalten.“[17]

In einem Snowden-Dokument mit der Überschrift „Special Source Operations Weekly“, datiert auf den 14. März 2013, ist zu lesen:

> „SSO was informed on 12 March 2013 that the access point for WHARPDRIVE was discovered by commercial consortium personnel. Witting partner personnel have removed the evidence and a plausible cover story was provided. All collection has ceased.”[18]

> „SSO wurde am 12. März 2013 benachrichtigt, dass der Zugriffspunkt für WHARPDRIVE von Mitarbeitern des kommerziellen Konsortiums entdeckt worden war. Scharfsinnige Mitarbeiter/innen des/der Partner/s entfernten alle Beweise und es wurde eine plausible Erklärung zur Verfügung gestellt. Sämtliche Erhebungen wurden eingestellt.“[19]

In einem am 16. Juni 2014 erschienenen Artikel schrieb *Der Spiegel* zu WHARPDRIVE:

---

17) Snowden-Dokument, MAT A Sek-4_gesamt, S. 3, auch Spiegel Online: So lesen Sie die NSA-Dokumente, 18.06.2014, http://www.spiegel.de/netzwelt/netzpolitik/glossar-noforn-sigdev-ts-so-lesen-sie-die-nsa-dokumente-a-975900.html.

18) Snowden-Dokument, MAT A Sek-4_gesamt, S. 208.

19) Übersetzung durch den Sprachendienst des Deutschen Bundestages.

> „Man habe angeboten, so heißt es in einem internen NSA-Papier, ein Team zusammenzustellen und das Equipment unauffällig wieder zu installieren.
>
> Die hochsensible Operation führte die NSA ganz offensichtlich nicht allein aus. Allem Anschein nach hatte sie dabei Hilfe aus Deutschland, genauer gesagt vom Bundesnachrichtendienst (BND). Der Deckname „Wharpdrive“ taucht in einem Dokument des Whistleblowers Edward Snowden über den anstehenden Besuch einer BND-Delegation in der NSA-Zentrale in Fort Meade auf. In den Instruktionen für den Besuch der Freunde aus Pullach heißt es: „Dankt dem BND für seine Hilfe bei dem trilateralen Programm.“ Und weiter wird ausgeführt, der deutsche Dienst habe bei der Überwachungsoperation die Führungsrolle inne, die NSA leiste technische Unterstützung.“[20]

Die Bundesregierung verweigerte jegliche Akten zur Operation WHARPDRIVE mit dem Hinweis, sie gehöre nicht zu den im Untersuchungsauftrag beschlossenen Themen des Ausschusses. Konkret hatte sie zu den entsprechenden Beweisbeschlüssen zur ‚Deutschland-Akte‘, BK-5 und BND-7, die Vollständigkeit der Aktenlieferung erklärt, ohne aber etwas zu WHARPDRIVE vorzulegen und auch ohne dies zu begründen. In der 19. Beratungssitzung am 6. November 2014 beschloss daher der Untersuchungsausschuss einstimmig, von der Bundesregierung eine schriftliche Begründung zu fordern,

> „[redacted]“[21]

Auch nach der dann abgegebenen schriftlichen Erklärung blieb die Opposition bei ihrer Auffassung, dass die Untersuchung von Operationen wie dieser zwischen NSA und

---

20) *Spiegel Online* vom 16. Juni 2014 „Eifer und Gier“, http://www.spiegel.de/spiegel/print/d-127626334.html, abgerufen am 29. Mai 2017.

21) Beratungsprotokoll-Nr. 19, S. 6.

BND und möglicherweise auch anderen Nachrichtendiensten zentrales Thema der Beweisaufnahme hätte sein müssen. Der Untersuchungsauftrag fragt explizit:

> „Waren Stellen des Bundes oder von ihnen mit sicherheitsrelevanten (auch IT-)Aufgaben Beauftragte Teil eines systematisierten wechselseitigen oder „Ring“-Tausches geheimdienstlicher Informationen, in dem der jeweils anderen Seite Daten oder Erkenntnisse übermittelt werden, die diese nach dem jeweils am Ort der Datenerhebung geltenden Recht selbst nicht erheben darf?“[22]

Bundesregierung und Koalition haben sich in ihrer Argumentation zum Ausschluss bestimmter Themen regelmäßig auf ein in den Untersuchungsauftrag eingebautes ‚Nadelör‘ berufen. Dort heißt es nämlich in Abschnitt B.I.:

> Der Untersuchungsausschuss soll (…) für den Zeitraum seit Jahresbeginn 2001 klären,
>
> I. ob, in welcher Weise und in welchem Umfang durch Nachrichtendienste der Staaten der sogenannten „Five Eyes“ (…) eine Erfassung von Daten über Kommunikationsvorgänge (…), deren Inhalte sowie sonstige Datenverarbeitungsvorgänge *von, nach und in*[23] Deutschland (…) erfolgte beziehungsweise erfolgt und inwieweit Stellen des Bundes, insbesondere die Bundesregierung, Nachrichtendienste oder das Bundesamt für Sicherheit in der Informationstechnik von derartigen Praktiken Kenntnis hatten, daran beteiligt waren, diesen entgegenwirkten oder gegebenenfalls daraus Nutzen zogen.[24]

Damit, so die Interpretation der Bundesregierung, habe der Bundestag sich selbst darauf festgelegt, nur solche Aktivitäten der Nachrichtendienste zu untersuchen, die sich

22) Antrag der Fraktionen CDU/CSU, SPD, DIE LINKE. Und Bündnis 90/Die Grünen „Einsetzung eines Untersuchungsausschusses“, Bundestagsdrucksache 18/843, Abschnitt B.I.7.

23) Eigene Hervorhebung.

24) Antrag der Fraktionen CDU/CSU, SPD, DIE LINKE. Und Bündnis 90/Die Grünen „Einsetzung eines Untersuchungsausschusses“, Bundestagsdrucksache 18/843, Abschnitt B.I.

auf digitale Kommunikation bezieht, die in Deutschland stattfindet oder zumindest ihren Anfangs- oder Endpunkt in Deutschland hat. Davon abgesehen, dass schon das Zustandekommen des Untersuchungsauftrags und später seiner Erweiterung maßgeblich von der Mehrheit im Parlament bestimmt wird, ist die Festlegung, wo sich digitale Kommunikationen im Internet vollziehen oder allein, von wo aus sie initiiert werden, nicht mehr mit absoluter Sicherheit möglich.[25]

Paketvermittelte Kommunikation – also alle Kommunikation, die digital transportiert wird, z. B. E-Mails, Internet-Telefonie, Chats oder Messenger – wird nicht immer auf dem kürzesten Weg durchs Internet transportiert. Benutzen ihre Teilnehmer_innen nicht-deutsche Dienste-Provider wie etwa *G-Mail* oder *Facebook*-Chats, und schützen sie sich zusätzlich etwa durch VPN-Dienste, ist es quasi unmöglich, ihre Kommunikation örtlich einzugrenzen.

bb) Gefangenenbefragung im US-Militärgefängnis in Bagram

Ebenfalls kategorisch für nicht-untersuchungsgegenständlich wurde ein Vorfall erklärt, der erst durch Zeugenaussagen in den Fokus des Ausschusses geraten ist.[26]

Am 4. Oktober 2010 wurden in Pakistan mehrere Personen durch eine US-amerikanische Kampfdrohne getötet, darunter der deutsche Staatsbürger *Bünyamin Erdogan*. Einen Tag vorher, am 3. Oktober, wurde ein weiterer Deutscher, *Ahmad Sidiqi*, im US-Militärgefängnis in Bagram, Afghanistan, von mehreren deutschen Beamten des Bundesamtes für Verfassungsschutz (BfV) verhört.[27] Unter den beteiligten Beamten war auch [redacted][28] Hintergrund der Befassung mit diesen Ereignissen war Punkt I.14. des Untersuchungsauftrags:

---

25) Vgl. Schriftliches Gutachten des Sachverständigen *Rechthien*, MAT A SV-13/3.

26) Vgl. hierzu Kapitel XII.4.e) – Verwendung von Daten aus Befragungen im Militärgefängnis Bagram für gezielte Tötungen?

27) *Die tageszeitung* vom 13. November 2010 „Aus dem Leben gebombt“.

28) Schreiben des Bundesministeriums des Innern vom 1. August 2016, MAT A BMI-25 (VS-NfD).

> „Haben US-amerikanische Stellen auf deutschem Staatsgebiet oder von diesem ausgehend Telekommunikationsüberwachungen, Festnahmen oder gezielte Tötungen durch Kampfdrohneneinsätze durchgeführt oder veranlasst? Welche Erkenntnisse lagen Stellen des Bundes zu welchem Zeitpunkt hierüber gegebenenfalls vor? Waren sie an der Vorbereitung oder Durchführung derartiger Maßnahmen gegebenenfalls in irgendeiner Form beteiligt oder haben sie gebilligt? (…)“[29]

Es lag also nahe, der Frage nachzugehen, ob es einen Zusammenhang zwischen der Befragung in einem für menschenverachtende Folterpraktiken bekannten US-Militärgefängnis[30] und dem Drohnenangriff einen Tag später gab, und insbesondere, ob möglicherweise Befragungsergebnisse oder sonstige Informationen an US-amerikanische Stellen übergeben wurden, die den Drohneneinsatz am nächsten Tag ermöglichten.

Die Bundesregierung allerdings versuchte Zeugenbefragungen zu dieser Thematik zu verhindern, in dem sie mehrfach kategorisch erklärte, es gebe keinen Zusammenhang zwischen der Befragung und Drohnenangriffen. Dem Zeugen *Isselburg* wurde mitgeteilt, er habe dazu keine Aussagegenehmigung.[31] Auch die Befragung des früheren BfV-Präsidenten *Heinz Fromm* zum Militärgefängnis in Bagram wurde durch den Vertreter des Bundesministerium des Innern (BMI) direkt mit der Bemerkung unterbrochen, er könne

> „(...) jetzt keinen Zusammenhang zum Untersuchungsgegenstand hier erkennen.“[32]

Zu den daraufhin auf Antrag der Opposition beschlossenen Beweisbeschlüssen, mit denen sämtliche Akten etc. im Zusammenhang mit der Befragung von *Ahmad Sidiqi*

---

29) Bundestagsdrucksache 18/843.

30) Zu Bagram auch bereits im Abschlussbericht des BND-Untersuchungsausschusses, 1. Untersuchungsausschuss der 16. Wahlperiode, Bundestagsdrucksache 16/13400, S. 110 ff.

31) *Isselburg*, Protokoll-Nr. 100 II – Auszug offen, S. 4

32) *Fromm*, Protokoll-Nr. 102 I, S. 47

beigezogen werden sollten, erklärten alle betroffenen Ministerien Fehlanzeige, also dass es keine den Untersuchungsauftrag betreffenden solchen Akten gebe.[33]

Auf Nachfrage erklärte der Vertreter des BMI die Fehlanzeige mit der Aussage des Zeugen Isselburg, denn der

> ‚[redacted]“.[34]

Es obliegt allerdings eben nicht den Zeug_innen oder der Bundesregierung, sondern dem Untersuchungsausschuss selbst zu prüfen, ob bestimmte Vorgänge dem Untersuchungsauftrag unterfallen. Der pauschale Hinweis der Bundesregierung, dem sei nicht so, reicht dabei nicht aus:

cc) Abschlussbericht SAW TAD

Im BfV wurde als Folge der Snowden-Enthüllungen eine zeitweilige Arbeitseinheit eingerichtet, die sich mit den Themen der Enthüllungen befasste, die ‚Sonderauswertung Technische Aufklärung durch US-amerikanische, britische und französische Nachrichtendienste‘ (SAW TAD). Laut Aussage des Leiters der SAW TAD bis April 2015 wurde die Arbeit dieser temporären Einheit im Frühjahr 2015 beendet.[35] Der Abschlussbericht der SAW TAD war nicht Teil der Akten, die dem Untersuchungsausschuss vorgelegt wurden. Begründung: Weil der Untersuchungszeitraum im März 2014 mit Einsetzung des Ausschusses endet. Dies begründet das BMI in einem Schreiben zur Erfüllung des Beweisbeschlusses BfV-24, mit dem der Abschlussbericht beigezogen werden sollte:

> ‚[redacted]

33) Beweisbeschlüsse BfV-25, BK-34, BMI-24, BND-62, BKA-3.

34) *MR Akmann* als Vertreter des BMI, Protokoll-Nr. 107, S. 5.

35) *Wingerath*, Protokoll-Nr. 98 I, S. 10.

> [redacted]
>
> [redacted]“[36]

Die Opposition hat diese Entscheidung kritisiert, weil die Themen des Abschlussberichts den im Ausschuss untersuchten Themen entsprechen und sich dabei aller Wahrscheinlichkeit nach auf den Untersuchungszeitraum beziehen. Auch wird der Bericht nicht erst mit dem Datum seiner Fertigstellung verfasst, sondern enthält Ergebnisse des gesamten Zeitraums der Existanz der SAW TAD, also ab Sommer 2013.

Zum maßgeblichen Zeitpunkt für die Erfasstheit durch den Beschluss eines Untersuchungsauftrages heißt es im Kommentar von Glauben/Brocker:

> „Solange nicht die Grenze erreicht ist, dass man bereits von einer unzulässigen entscheidungsbegleitenden Kontrolle der Exekutive sprechen müsste, ist es nicht erforderlich, im Verfahren als zeitliche Zäsur zwingend den Tag des letzten vom Plenum beschlossenen Einsetzungsantrages abzustellen. In der Regel werden nämlich solche Sachverhalte, die in einem inneren sachlogischen Zusammenhang mit dem Untersuchungsgegenstand stehen, durch den Untersuchungsauftrag zumindest stillschweigend vorausgesetzt und sind daher auch mit umfasst. Die Befugnisse des UA können sich daher auch grundsätzlich auch auf Vorgänge erstrecken, die zeitlich nach dem Einsetzungsbeschluss des Plenums liegen sowie auch auf Unterlagen, die erst später entstanden sind.“[37]

---

36) Schreiben des BMI zum Beweisbeschluss BfV-24 vom 22. Juli 2016, MAT A BfV-24 (VS-NfD).

37) *Glauben/Brocker*, Das Recht der parlamentarischen Untersuchungsausschüsse in Bund und Ländern, 2016, S. 179.

Die Beschränkung auf das vom BMI dann vorgeschlagene „Treptow-Verfahren“, bei dem lediglich die Abgeordneten den Bericht in der Dienststelle des BfV in Treptow einsehen können, in diesem konkreten Fall von Ende Juli bis Ende Oktober 2016,[38] hat die Opposition erheblich behindert.

dd) Vorlage „ohne Anerkennung einer Rechtspflicht“

Die Bundesregierung hat in einer ganzen Reihe von Fällen dem eigenen Selbstverständnis nach großzügig darüber hinweggesehen, dass bestimmte durch Beweisbeschlüsse beigezogene Akten in ihrem Verständnis nicht vom Untersuchungsauftrag umfasst seien und sie in Einzelfällen vorgelegt, teils nur zur Einsicht, nur in Räumlichkeiten der Nachrichtendienste oder im Kanzleramt und dabei oft nur für die Abgeordneten, nicht aber deren Mitarbeiter_innen.

Die Vorlage „ohne Anerkennung einer Rechtspflicht“ macht es dem Ausschuss im Übrigen unmöglich nachzuvollziehen, ob die betreffenden Akten vollständig sind oder ob sie ein völlig falsches Bild vom Sachverhalt abbilden, weil relevante Teile möglicherweise fehlen.

Dabei handelt es sich um eine völlig inakzeptable Beschränkung. Im oben bereits zitierten Urteil des Bundesverfassungsgerichts heißt es:

> „Der Untersuchungsausschuss muss sich nicht mit Aktenauskünften zufrieden geben oder sein Verlangen auf bestimmte Aktenteile beschränken. Vielmehr soll er sich anhand der vollständigen Akten selbst ein Bild vom Umfang ihrer Entscheidungserheblichkeit machen können (vgl. BVerfGE 67, 100 <128 ff.>). Der Vorlageanspruch bezieht sich grundsätzlich auf alle Akten, die mit dem Untersuchungsgegenstand in Zusammenhang stehen. Bei einem Ersuchen auf Aktenvorlage muss nicht bereits feststehen, dass die Unterlagen auch tat-

38) Schreiben des BMI zum Beweisbeschluss BfV-24 vom 22. Juli 2016, MAT A BfV-24 (VS-NfD).

> sächlich entscheidungserhebliches Material oder entsprechende Beweismittel enthalten. Es reicht aus, wenn sie Hinweise hierauf geben könnten.“[39]

c) Zeugen haben Akten, bevor sie dem Ausschuss übergeben werden

Bereits in einer der ersten öffentlichen Zeugen-Vernehmungen im Herbst 2014 kam es kurz nach Beginn zum Abbruch einer Sitzung, weil sich herausstellte, dass dem Zeugen Akten vorlagen, die der Ausschuss zwar angefordert, aber noch nicht erhalten hatte.[40] Dass Zeug_innen, die selbst Mitarbeiter_innen von Behörden oder Ministerien sind, für ihre Vorbereitung Akten einsehen können, gehört zum üblichen Verfahren der Untersuchung. Ausgesprochen problematisch ist aber, dass die Mitglieder des Untersuchungsausschusses die Akten zu spät und mit umfangreichen Schwärzungen erhalten, während die zu befragenden Zeug_innen die Akten ungeschwärzt einsehen können.

Eine sachgerechte Befragung ist nicht möglich, wenn Zeugen vor ihrer Vernehmung Zugang zu Akten haben, die dem Ausschuss nicht vorliegen.

d) Bundesregierung „findet“ Akten

Im Februar 2015 erklärte der Zeuge R.S. in eingestufter Sitzung, er habe zur Vorbereitung seiner Aussage Akten eingesehen, bei denen bei näherer Beschreibung der Eindruck entstand, dass sie dem Ausschuss nicht vorgelegt worden waren.[41] Die Bundesregierung wurde aufgefordert, dies zu prüfen und teilte dem Ausschuss einige Tage später mit:

---

39) BVerfGE 124, 78, zitiert nach http://www.bverfg.de/e/es20090617_2bve000307.html, dort Rn. 113

40) *T. B.*, Protokoll-Nr. 18 I, S. 17f.

41) *R. S.*, Protokoll-Nr. 37 II – Auszug offen, S. 31

> „Der Bundesnachrichtendienst hat heute aufgrund einer ersten Bewertung mitgeteilt, dass etwa 130 Dokumente, die unter die Beweisbeschlüsse BND-19/21 fielen, aufgrund eines Versehens dem Untersuchungsausschuss bislang nicht übermittelt worden seien.“[42]

Ob es weitere solche zurückgehaltenen Akten gab, war für den Ausschuss nicht nachprüfbar, es erscheint aber jedenfalls unglaubwürdig, dass ausgerechnet bei einer Operation des BND mit einem US-Nachrichtendienst, die so sensibel ist, dass die Bundesregierung darauf beharrte, dass ihr – in der Presse veröffentlicher – Name im Ausschuss nicht ausgesprochen werden dürfe, über hundert Unterlagen unbeabsichtigt übersehen wurden.

e) Zurückgehaltene Akten: Der Beweisbeschluss BND-26

Obwohl der Ausschuss durch weit formulierte Beweisbeschlüsse zu Beginn der Untersuchung darauf zielte, sämtliche vom Untersuchungsauftrag umfassten Akten beizuziehen, legte die Bundesregierung wesentliche Aktenteile erst zu spät vor. Das herausstechende Beispiel sind die Akten, die letztlich zum ‚Selektoren-Skandal‘ führten.[43]

Im April 2014 beschloss der Ausschuss, sämtliche Akten beizuziehen,

> „die die Fragestellungen der Abschnitte I. und II des Untersuchungsauftrags mit Ausnahme der Fragen 1.13. bis 1.15. und 11,4 betreffen, und die im Organisationsbereich des Bundesnachrichtendienstes nach dem 1. Juni 2013 entstanden (…) sind“.[44]

Damit waren etwa die Fragen umfasst, ob und wie die NSA Daten oder deren Inhalte in Deutschland erfasst, ob und was die Bundesregierung und ihre Behörden darüber wussten, gegen welche Gesetze dabei ggbf. verstoßen wurde oder ob sich solche Aktivitäten gegen deutsche Unternehmen richteten.

---

42) Schreiben des Bundeskanzleramts an das Sekretariat des 1. PUA vom 3. März 2015, MAT A BND-19/4 und BND-21/3

43) Vgl. hierzu Kapitel V.8 – Verstöße bei der Verwendung von Suchbegriffen/Selektoren der NSA und Kapitel IX. – „No Spy“ und Pofallas Erklärung.

44) Beweisbeschluss BND-1.

Von problematischen, weil gegen deutsche und europäische Interessen verstoßenden Suchbegriffe (auch: ‚Selektoren') der NSA, die vom BND in vom BND erfassten Kommunikationsdaten eingesetzt wurden, erfuhr der Ausschuss allerdings erst, nachdem im Februar 2015 der 26. BND-Beweisbeschluss beschlossen wurde, mit dem Akten beigezogen wurden, die

> „Auskunft darüber geben, welche Erkenntnisse beim Bundesnachrichtendienst darüber vorlagen oder vorliegen, inwiefern die National Security Agency im Rahmen der Zusammenarbeit in der Joint SIGINT Activity Aufklärung gegen deutsche Ziele oder deutsche Interessen (d. h. gegen Menschen in Deutschland oder der EU; (…) oder entsprechen gegen Unternehmen (…) versucht oder tatsächlich betrieben hat und wie deutsche Behörden darauf reagierten."[45]

Diese Akten hätte die Bundesregierung bereits im Sommer 2014 vorlegen müssen.

f) Einstufungen

aa) Einstufungen von Akten

Die Arbeit des Untersuchungsausschusses wurde erheblich und in unnötiger Weise durch die Einstufungspraxis der Bundesregierung behindert. Verschiedene Akten konnten von Abgeordneten, nicht aber ihren Mitarbeiter_innen eingesehen werden. In anderen Fällen konnten lediglich die Obleute der Fraktionen im Ausschuss die Akten einsehen. Die Abgeordneten mussten dazu verschiedene Orte außerhalb des Deutschen Bundestages aufsuchen:

- Die BND-Dienststelle im Gardeschützenweg in Berlin-Lichterfelde
- Die BND-Dienststelle in Berlin-Treptow
- Die BND-Dienststelle in der Chausseestraße in Berlin-Mitte
- Das Bundeskanzleramt.

45) Beweisbeschluss BND-26.

Die Abgeordneten durften teils keinerlei Notizen machen und waren also darauf angewiesen, relevante Details auswendig zu lernen. In anderen Fällen war es möglich, handschriftliche Notizen zu machen, allerdings mussten diese dann der Bundesregierung zur Aufbewahrung übergeben werden. Diese brachte die Notizen dann zu den relevanten Zeugenbefragungen mit.

Die Aufgabe des Untersuchungsausschusses ist es, eine Ermittlung auch gegen die Bundesregierung durchzuführen. Wenn die Kontrolle der Arbeitsmaterialien der Untersuchung dann aber in den Händen der Untersuchten liegt, führt das den gesamten Prozess ad absurdum.

aaa) Die Einstufung des Berichts über den Kontrollbesuch des/der BfDI in Bad Aibling

Die Auseinandersetzung zwischen dem Ausschuss und der Bundesregierung über die Übergabe des Berichts der Bundesbeauftragten für die Informationsfreiheit und den Datenschutz (BfDI) über den BfDI-Kontrollbesuch in der BND-Dienststelle Bad Aibling im Dezember 2013 und Oktober 2014 steht exemplarisch für die Blockade-Haltung der Bundesregierung.

Der Ausschuss hat die Beiziehung des Berichts der BfDI am 10. September 2015 beschlossen[46], und zunächst den teilweise geschwärzten und im Übrigen streng geheim eingestuften Sachstandsbericht zum Kontrollbesucht erhalten[47]. Die rechtliche Bewertung der vorgefundenen Fakten durch die BfDI wurde dem Kanzleramt für die Erstellung einer Stellungnahme übermittelt. Der Ausschuss erhielt die Bewertung der BfDI im März 2016[48], wobei das Kanzleramt der Meinung war, sie könne ohne Vorliegen der Stellungnahme von BND bzw. Kanzleramt und ggbf. deren Einarbeitung in die Bewertung gar nicht als fertiggestellt gelten und daher dem Ausschus auch nicht übermittelt werden. Die Bewertung wurde ‚geheim' eingestuft, was von der Opposition massiv kritisiert wurde, da zumindest ein Teil der so eingestuften Inhalte der Bewertung an

46) Beweisbeschluss BfDI-8.

47) Übersendungsschreiben der BfDI vom 21. September 2015 zur Übersendung des Sachstandsberichts, MAT A BfDI-8/2 (Tgb.-Nr. 44/15 – STRENG GEHEIM) (ohne Anlagen VS-NfD).

48) Rechtsbewertung der BfDI, MAT A BfDI-8/5 (Tgb.-Nr. 242/16 – GEHEIM).

anderer Stelle im Bericht der „Vertrauensperson der Bundesregierung“[49], *Dr. Kurt Graulich* über die NSA-Selektoren vom November 2015 überhaupt nicht eingestuft sind.[50] Der Bericht der „Vertrauensperson der Bundesregierung“ kommt allerdings in Teilen zu ganz anderen Bewertungen.

Der Ausschuss hatte die BfDI dann im April um eine eine herabgestufte Fassung der Bewertung mit punktuellen Schwärzungen gebeten[51]. Dies war letztlich aber nicht möglich, weil die Einstufung vom Kanzleramt vorgegeben war, da die Bewertung sich auf Unterlagen des BND bezieht und die jeweils einstufende Stelle weiterhin über die Einstufungspraxis entscheidet: In diesem Fall also das Kanzleramt für den BND. Damit waren der BfDI die Hände gebunden.[52]

Dies setzte sich fort beim Versuch, die Stellungnahme des BND und des Kanzleramts zur BfDI-Bewertung beizuziehen. Die Mehrheit vertagte den entsprechenden Beweisantrag der Opposition[53] vor der Sommerpause 2016 auf die Sitzung nach der Sommerpause, die Stellungnahme des Kanzleramts erreicht den Ausschuss – ohne Anerkennung einer Rechtspflicht und nur zur Einsicht in der Geheimschutzstelle des Bundestages – Ende September 2016[54], die Reaktion der BfDI darauf Ende Oktober[55].

Das Blog netzpolitik.org hatte die Bewertung unterdessen im September 2016 vollständig veröffentlicht.[56]

---

49) Vgl. hierzu in diesem Kapitel unter 2.i) „Die Einsetzung der „Vertrauensperson der Bundesregierung“ Graulich“.

50) Graulich: Bericht „Nachrichtendienstliche Fernmeldeaufklärung mit Selektoren in einer transnationalen Kooperation“ vom 23. Oktober 2015, MAT A SV-11/2.

51) Beratungsprotokoll-Nr. 93, S. 4.

52) Beratungsprotokoll-Nr. 95, S. 5 und Schreiben der BfDI an den Untersuchungsausschuss vom 30. Juni 2016, MAT A BfDI-8/5_1 (VS-NfD).

53) Beratungsprotokoll-Nr. 105, S. 6 ff.

54) Stellungnahme des Kanzleramts zum BfDI-Prüfbericht, (Tgb-Nr. 281/16 – GEHEIM).

55) Erwiderung der BfDI auf die Stellungnahme des Bundeskanzleramts zur Rechtsbewertung der BfDI am 12. Oktober 2016, MAT A BfDI-8/7 (Tgb.-Nr. 285/16 – GEHEIM).

56) netzpolitik.org vom 1. September 2016 „Geheimer Prüfbereicht: Der BND bricht dutzendfach Gesetz und Verfassung – allein in Bad Aibling (Updates). Abrufbar unter https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/.

In der Gesamtbetrachtung drängt sich die Vermutung auf, der Umgang mit dem Bericht der BfDI könnte vor allem das Ziel verfolgt haben, durch Verzögerung, Einstufungen und Schwärzungen eine der Bundesregierung unangenehme Bewertung der Praxis des BND der parlamentarischen Kontrolle durch den Untersuchungsausschuss und darüber hinaus der Öffentlichkeit möglichst zu entziehen.

bb) Einstufungen von Ausschuss-Sitzungen

Die inflationäre Einstufung von Ausschusssitzungen als geheim und auch streng geheim ist zu kritisieren. Gerade die später teilweise auf ‚offen' herabgestuften Protokolle belegen, dass Vieles, was in eingestuften Sitzungen zur Sprache kam, mit den Zeug_innen auch in öffentlichen Vernehmungen hätte besprochen werden können und müssen.

Es hat sich gezeigt, dass Zeug_innen häufig in eingestuften, nicht-öffentlichen Sitzungen ein völlig anderes Aussageverhalten an den Tag gelegt haben. Nachdem sich dieses Muster wiederholte, hätte die Bundesregierung in der Beratung der Zeug_innen darauf dringen können, auch öffentlich mehr zu berichten.

cc) Aussagegenehmigungen

Zeug_innen, die zugleich Amtsträger_innen sind (also bspw. Mitarbeiter_innen der Nachrichtendienste oder Ministerien), müssen bei einer Vernehmung durch den Untersuchungsausschuss ihre dienstliche Verschwiegenheitsverpflichtung beachten. Deshalb ist die Bundesregierung zur Erteilung der erforderlichen Aussagegenehmigung verpflichtet (§ 23 Abs. 2 Untersuchungsausschussgesetz – PUAG). Die seitens der Bundesregierung erteilten Aussagegenehmigungen waren allerdings unter verschiedenen Gesichtspunkten fehlerhaft oder mindestens kritikwürdig.

So hat die Bundesregierung in einigen Fällen bereits von sich aus festgelegt, dass Zeugen ausschließlich in nichtöffentlicher Sitzung vernommen würden. § 14 PUAG legt aber fest, dass, falls erforderlich, der Ausschuss diese Entscheidung trifft und der (oder die) Vorsitzende dies in öffentlicher Sitzung begründet, denn grundsätzlich gilt „Die Beweiserhebung erfolgt in öffentlicher Sitzung" (§13 (1) PUAG).

Den Zeug_innen wurde mit der Aussagegenehmigung durch die Bunderegierung mitgeteilt, dass Grundlage ihrer Vernehmung nicht nur der Untersuchungsauftrag und der jeweilige Beweisbeschluss, sondern auch die Begründung der zugehörigen Beweisanträge sei. Tatsächlich haben aber nur sehr wenige Beweisanträge überhaupt eine Begründung enthalten, da dies keine förmliche Voraussetzung ist und auch ausschließlich(!) der Willensbildung der Ausschussmitglieder dient. Die Aussagegenehmigungen wurden so unzulässig eingeschränkt, wenn der dem Beweisbeschluss zugrundeliegende Beweisantrag sich auf den gesamten Untersuchungsauftrag bezog, die Begründung aber eine Schwerpunktsetzung enthielt oder beispielhaft einzelne Punkte des Untersuchungsauftrages erwähnte.

Weiter wurde den Zeug_innen mitgeteilt, dass sich die Aussagegenehmigung nur auf zum Zeitpunkt des Einsetzungsbeschlusses abgeschlossene Sachverhalte erstrecke. Dies verkürzt das parlamentarische Untersuchungsrecht unzulässigerweise, denn die parlamentarische Kontrolle bezieht sich auch auf Vorgänge, die noch nicht abgeschlossen sind, wenn sie zumindest Verantwortungsreife erreicht haben.[57] Die Auffassung der Bundesregierung hätte beispielsweise Vernehmungen zum Komplex „Geheimer Krieg“ in Abschnitt B.I.13. und 14. des Untersuchungsauftrages verhindert.

Den Zeug_innen wurde auferlegt, selbst eine Abwägung zwischen dem parlamentarischen Aufklärungsrecht und dem etwaig betroffenen Wohl des Bundes (Staatswohl) vorzunehmen. Eine fehlerhafte und infolgedessen in der Sache rechtswidrige Entscheidung der Zeug_innen in der einen wie der anderen Richtung (Aussage trotz Überwiegens der Belange des Bundes, keine Aussage trotz Überwiegens des Aufklärungsrechtes des Parlamentes im Einzelfall) bringt die Zeug_innen in die Gefahr, sich im Ergebnis rechtswidrig zu verhalten, ggf. sogar wegen Geheimnisverrats strafbar zu machen. Mit der Obhutspflicht als Dienstherrin ist eine solche Aussagegenehmigung daher nicht zu vereinbaren. Schließlich legte die Bundesregierung fest, dass im Zweifel eine Aussage unterbleiben müsse, was im Widerspruch zu Artikel 44 Grundgesetz (GG) steht.

---

57) *Gärditz* in *Waldhoff/Gärditz*, PUAG, § 18, Rz. 33 m. w. N.

Im Kern lässt sich festhalten, dass auch die erteilten Aussagegenehmigungen die Arroganz der Bundesregierung in Zeiten der Großen Koalition illustrieren. In ihr steckt der Anspruch, allein zu entscheiden, was das Parlament wie untersuchen und kontrollieren dürfe. Dass sich die Koalitionsmehrheit dieser Haltung nicht selten angeschlossen hat, hat mit dazu beigetragen, dass die Untersuchung in vielen Punkten lückenhaft geblieben ist.

dd) Schwärzungen von Akten und Protokollen

Neben den Einstufungen und Beschränkungen der Einsichtnahme hat die Bundesregierung die Akten in großem Umfang geschwärzt. Das Bundesverfassungsgericht hat in seinem Urteil zur Klage der Opposition im BND-Untersuchungsausschuss 2007 dazu festgestellt:

> „Sollen einem Untersuchungsausschuss Unterlagen unter Berufung auf Art. 44 Abs. 2 Satz 2 GG vorenthalten werden, bedarf dies daher einer Begründung, die (…) substantiiert auch darlegt, warum die erhobenen Informationen einem Verbot der Verwertung durch den Ausschuss unterliegen sollen.“[58]

Zwar hat die Bundesregierung jeder Akte eine bis zu siebenseitige pauschale Erläuterung der Gründe der jeweiligen Schwärzungen vorangestellt. Aber eine pauschale Begründung entspricht eben genau nicht der erforderlichen Darlegungslast.

Es ist von allen Fraktionen moniert worden, dass in Protokollen geheim eingestufter Sitzungen auch Fragen von Abgeordneten geschwärzt wurden. Das wäre nachvollziehbar in Fällen, bei denen die Frage selbst auch eingstufte Inhalte erwähnt. Es gab aber auch Fälle, in denen das überhaupt nicht der Fall war.

So fragte beispielsweise die Abgeordnete *Martina Renner* in der 77. Ausschusssitzung den Zeugen *A.Sch.*

58) BVerfGE 124, 78, zitiert nach http://www.bverfg.de/e/es20090617_2bve000307.html, dort Rn. 181.

> „Kommen denn die Metadaten der Kontaktperson auch in die Verarbeitung durch XKeyscore?“

Diese Frage wurde in der von der Bundesregierung freigegebenen Fassung des Protokolls geschwärzt und noch viele weitere.[59] In einer der folgenden Beratungssitzungen wurde diese Schwärzungspraxis kritisiert und dabei insbesondere auch die Schwärzungen von Fragen. Erst nach einer detaillierten Auflistung[60] war die Ausschussmehrheit bereit, sich mit dem Problem zu befassen. Das Resultat war, dass die Bundesregierung in einigen Fällen bereit war, die Schwärzungen aufzuheben, in anderen nicht.[61] Es ist allerdings der Opposition mit nicht nur einem Viertel der Abgeordneten im Ausschuss, sondern auch auch nur einem Viertel der Mitarbeiter_innen und sonstigen Ressourcen nicht möglich, jede Schwärzung in dieser Form einzeln zu überprüfen.

Die Bundesregierung ging dabei offensichtlich nach dem Prinzip „Im Zweifel schwärzen“ vor, und die Zweifel dem Bundestag gegenüber waren zahlreich. Für eine sinnvolle Kontrolle der Regierung durch das Parlament muss allerdings das Gegenteil gelten: „Im Zweifel nicht schwärzen“, denn, auch das hat das Verfassungsgericht explizit festgehalten:

> „Für die Beantwortung der Frage, ob Zeugenaussagen oder die Vorlage von Akten das Staatswohl gefährden würden, ist danach zunächst zu berücksichtigen, dass der Umgang mit Informationen in einem Untersuchungsausschuss eigenen Geheimschutzbestimmungen unterliegt (vgl. BVerfGE 67, 100 <135>), und dass das Staatswohl nicht allein der Bundesregierung, sondern dem Bundestag und der Bundesregierung gemeinsam anvertraut ist. Das Parlament und seine Organe können nicht als Außenstehende behandelt werden, die zum

59) Martina Renner, MdB DIE LINKE., Protokoll-Nr. 77 II – Auszug öffentlich.

60) Schreiben von Martina Renner, MdB DIE LINKE., an Bundeskanzleramt und Bundesministerium des Innern vom 15. März 2016, Ausschussdrucksache 468.

61) Beratungsprotokoll-Nr. 90, S. 4 f.

> Kreis derer gehören, vor denen Informationen zum Schutz des Staatswohls geheimzuhalten sind.“[62]

Zwar gibt es neben dem Schutz des Staatswohls noch eine Reihe anderer pauschaler Begründungen für Schwärzungen. Sie alle erfordern aber eine spezifische Erläuterung.[63]

ee) Die „Clearingstelle“

Bereits die ersten Akten, die die Bundesregierung dem Ausschuss übergab, waren umfangreich geschwärzt. Das sogenannten „Clearingstellen-Verfahren“ zwischen dem Ausschuss und der Bundesregierung zur Entschwärzung bzw. Herausgabe von Akten war allerdings nicht praktikabel, weil es für den Ausschuss auf Dauer nicht zu bewältigen war.

Bereits in der 10. Sitzung des Ausschusses wurde berichtet,

> „[redacted][64]

Nach der ersten Besprechung auf Arbeitsebene waren sich die Fraktionen einig, dass die sogenannte ‚Clearingstelle‘ zu Erörterung der Notwendigkeit von Aktenschwärzungen keine dauerhafte Einrichtung sein könne. Selbst der Obmann der CDU/CSU-Fraktion, *Roderich Kiesewetter*, hielt in der folgenden Beratungssitzung fest

> „[redacted]

62) BVerfGE 124, 78, zitiert nach http://www.bverfg.de/e/es20090617_2bve000307.html, dort Rn. 130.

63) Vgl. hierzu Kapitel V.6 – Ungelöste Filterproblematik.

64) Beratungsprotokoll-Nr. 10, S. 5.

[redacted]“[65]

Das Verfahren wurde noch im Oktober fortgesetzt, dann aber abgebrochen, weil gerade den kleineren Oppositionsfraktionen die Kapazitäten hierfür fehlten. Grund zur Kritik an der umfangreichen Schwärzungspraxis gab es weiterhin.

g) Konsultationsverfahren und Third-Party-Rule

Große Teile des Untersuchungsauftrags konnten nicht bzw. nicht angemessen untersucht werden, weil die Bundesregierung die meisten Akten mit Bezug zu den Staaten der Five Eyes zurückhielten. Sie sieht sich durch Vereinbarungen zwischen Nachrichtendiensten wie etwa das Memorandum of Agreement von 2002[66] gebunden, die festlegen, dass beide Partner zustimmen müssen, bevor Informationen über die in den Vereinbarungen festgelegten Kooperationen an Dritte weitergegeben werden können.[67] Der Bundestag wird so als ‚Dritter‘ definiert, mit der Folge, dass die Bundesregierung die Zustimmung bspw. der US- oder der britischen Regierung einholt, bevor sie Unterlagen über möglicherweise rechtswidrige Aktivitäten deutscher Nachrichtendienste an einen parlamentarischen Untersuchungsausschuss übergibt.

‚[redacted] „5-

65) Beratungsprotokoll-Nr. 12, S. 9.

66) dazu siehe unter V.1 – MoA von 2002.

67) Beratungsprotokoll-Nr. 12, S. 4 f.

[redacted][68]

Das bezieht sie sogar auf Akten, die durch deutsche Stellen erstellt wurden:

‚[redacted].“[69]

Selbst die Vereinbarungen, die die Grundlagen der konkreten Kooperationen darstellen – häufig als ‚Memorandum of Understanding‘ (MoU) oder ‚Memorandum of Agreement‘ (MoA) bezeichnet –, unterliegen der Konsultation. So erklärte der Vertreter des BMI im Ausschuss:

‚[redacted]“[70]

Für die gesamte Dauer des Untersuchungsausschusses wurde so verfahren: nicht nur die Suchbegriffe der NSA, mit denen der BND die von ihm erfassten Daten durchsucht, konnten so vom Untersuchungsausschuss nicht untersucht werden, sondern darüber hinaus zahlreiche weitere im Kontext der Snowden-Enthüllungen.

Die parlamentarische Kontrolle wird so ad absurdum geführt: Die Bundesregierung bzw. ihre Nachrichtendienste schließen – geheim eingestufte – Verträge mit den Re-

68) Staatssekretär *Klaus-Dieter Fritsche*, Beratungsprotokoll-Nr. 12 (Wortprotokoll), S. 2.

69) Staatssekretär *Klaus-Dieter Fritsche*, Beratungsprotokoll-Nr. 12 (Wortprotokoll), S. 2.

70) Beratungsprotokoll-Nr.10, S. 5.

gierungen bzw. Nachrichtendiensten anderer Staaten ab. Ob und was das die Bundesregierung kontrollierende Parlament davon erfährt, entscheiden also weder Bundestag noch Bundesregierung, sondern die Regierung eines anderen Staates.

Ein Effekt dieser Vorgehensweise war im Übrigen, dass Akten nicht rechtzeitig zu den relevanten Zeugenvernehmungen vorgelegt wurden, weil die Konsultation nicht abgeschlossen war.

Der Beauftragte des Bundes, Staatssekretär Klaus-Dieter Fritsche, macht zur Third-Party-Rule auch Ausführungen in seiner Stellungnahme zur Bewertung der BfDI zu deren Kontrollbesuch in Bad Aibling 2013 und 2014.[71]

h) Die Bedeutung der Entscheidung des BVerfG zu NSA-Selektoren für die parlamentarische Kontrolle von Nachrichtendiensten

Zur näheren Würdigung des Beschlusses des Bundesverfassungsgerichts zur Nicht-Herausgabe der von deutschen Behörden eingesetzten Selektoren an den Untersuchungsausschuss[72] weisen die Oppositionsfraktionen auf den erhellenden Aufsatz von Christoph Möllers[73] hin. Denn es ist nicht ihre Aufgabe, im Rahmen eines Untersuchungsausschussberichts die Rechtsprechung des Bundesverfassungsgerichts zu durchleuchten. Die Oppositionsfraktionen merken jedoch an, dass sie es für demokratiepolitisch problematisch halten, wenn die Zusammenarbeit der internationalen Geheimdienste auch aufgrund von Verwaltungsabkommen und unverbindlichen Absprachen, die ohne Zustimmung des Parlamentes getroffen werden, letztlich dazu führen, dass die Tätigkeit deutscher Geheimdienste durch das deutsche Parlament nicht mehr selbst kontrolliert werden kann. In den Blick zu nehmen sein wird daher in der nächsten Legislaturperiode, ob auf der Linie des 1. Senats des Bundesverfassungsgerichts ein

---

71) Stellungnahme des Kanzleramt vom 28. September 2016, MAT A BK-(A-Drs. 512) (Tgb.-Nr. 281/16 – GEHEIM).

72) BVerfG, Beschluss des Zweiten Senats vom 13. Oktober 2016 – 2 BvE 2/15 –, abrufbar unter http://www.bverfg.de/e/es20161013_2bve000215.html,

73) *Möllers, Christoph*: Von der Kernbereichsgarantie zur exekutiven Notstandsprärogative: zum BND-Selektoren-Beschluss des BVerfG, JuristenZeitung 2017, S. 271-278; ähnlich: von Achenbach, Jelena; Nešković, Wolfgang: Selektoren-Urteil des BVerfG: Karlsruhe verzwergt das Parlament, Verfassungsblog, 2016/11/21, abrufbar unter http://verfassungsblog.de/selektoren-urteil-des-bverfg-karlsruhe-verzwergt-das-parlament/,

noch strengeres „Bestimmtheitsregime“[74] für die internationale Geheimdienstzusammenarbeit deutscher Geheimdienste verankert werden kann, das auch die parlamentarischen Kontrollrechte stärkt.

i) Die Einsetzung der „Vertrauensperson der Bundesregierung“ Graulich

Die Mehrheit hat sich im Juli 2015 selbst und damit den Ausschuss insgesamt der Möglichkeit beraubt, die durch den Beweisbeschluss BND-26 zunächst dem Ausschuss und dann der Öffentlichkeit bekannt gewordenen NSA-Selektoren zu untersuchen.

Die Bundesregierung verweigerte dem Ausschuss die Einsicht mit dem Argument, diese müsse mit der US-Regierung konsultiert werden und die US-Regierung hatte die Einsicht abgelehnt. Am Ende ihrer Überlegungen stand der Vorschlag, eine sogenannte „Vertrauensperson der Bundesregierung“ oder ‚unabhängige sachverständige Vertrauensperson‘ solle die Selektoren einsehen und dem Ausschuss darüber berichten.

Die „Vertrauensperson der Bundesregierung“ *Dr. Kurt Graulich* erklärte noch vor seiner Einsetzung in einem Interview, wem er sich verpflichtet fühlte:

> „Ich werde meine Aufgabe loyal gegenüber dem Auftraggeber erfüllen. Das ist in diesem Fall die Bundesregierung.“[75]

Einen Tag später beschloss die Ausschussmehrheit seine Einsetzung.[76]

Für die Opposition war und ist dieses Verfahren nicht akzeptabel. Es umgeht die Regeln des PUAG gleich mehrfach: *Dr. Kurt Graulich* wurde bereits im Beweisbeschluss zum ‚Sachverständigen‘ erklärt, mit dem später eine Anhörung stattfinden sollte. Ein Sachverständiger war und ist *Dr. Kurt Graulich* aber genau nicht, genausowenig wie

---

74 *Möllers, Christoph*: Von der Kernbereichsgarantie zur exekutiven Notstandsprärogative: zum BND-Selektoren-Beschluss des BVerfG, JuristenZeitung 2017, S. 271 (274).

75) *Spiegel Online* vom 1. Juli 2015 „Designierter NSA-Sonderermittler. Ein Mann, 40.000 brisante Daten“, abrufbar unter http://www.spiegel.de/politik/deutschland/nsa-sonderermittler-kurt-graulich-ein-mann-40-000-datensaetze-a-1040661.html.

76) Beratungsprotokoll-Nr. 56, S. 6 und Ausschussdrucksache 385

ein im Untersuchungsausschuss sonst üblicher Sonderermittler. In beiden Fällen ersetzt er nicht die Einsicht in die Beweismittel. Im konkreten Fall der NSA-Selektoren ging es aber genau darum: die Beweiserhebung durch den Ausschuss durch ein frei erfundenes Verfahren zu ersetzen, das dem PUAG nicht genügt, und das im Übrigen auch weder im Recht des Parlamentarischen Kontrollgremiums noch in der Geschäftsordnung des Bundestages zu finden ist.

Die Bundesregierung hat hier mit Unterstützung der Mehrheit im Ausschuss die Kontrolle des Parlaments außer Kraft gesetzt.

Dies zeigte sich im Besonderen durch die spezifischen Umstände der Untersuchung der NSA-Selektoren durch die „Vertrauensperson der Bundesregierung“:

Dr. Kurt Graulich arbeitete in den Räumen des BND in der Chausseestraße, wurde dort von BND-Mitarbeiter_innen – und nur solchen – unterstützt und verfasste schließlich ein Gutachten, dass in Teilen vom BND abgeschrieben war.

> „Der Sondergutachter der Bundesregierung für die NSA-Selektoren, Kurt Graulich, hat im NSA-Untersuchungsausschuss zunächst bestätigt, Teile seiner rechtlichen Einschätzung für seinen Abschlussbericht aus Schriftstücken des Bundesnachrichtendienstes übernommen zu haben. „Ich habe die schriftliche Version eines Textes vertreten, die ganz gut zusammenschrieb, was für den Zweck hier taugt“, sagte er.“[77]

Im Übrigen ist ein „Konsultationsverfahren“ nicht gleich zu setzen mit der Einräu-mung eines Vetos. Konsultieren bedeutet lediglich, der anderen Seite die Möglichkeit einzuräumen, zur möglichen Weitergabe der Unterlagen Stellung zu nehmen. Selbst wenn der Konsultierte dagegen ausspricht, trifft die Entscheidung die konsultierende Seite, also hier die Bundesregierung. Wie sich die USA im Konsultationverfahren tatsächlich geäußert hatten, ob und wie strikt sie gegen eine Weitergabe waren, ist nicht bekannt.

77) *Süddeutsche Zeitung Online* vom 5. November 2015, „Sonderermittler Graulich bestreitet Einflussnahme durch BND“, abrufbar unter http://www.sueddeutsche.de/politik/nsa-ausschuss-sonderermittler-graulich-bestreitet-einflussnahme-durch-bnd-1.2724470.

Ob die USA tatsächlich gefordert haben, dass die NSA-Selektoren dem Untersuchungsausschuss des deutschen Parlaments nicht vorgelegt werden dürften, ist letztlich nicht geklärt. Jedenfalls ist kaum vorstellbar, dass in den USA einem Ausschuss des US-Kongress solche Unterlagen verweigert worden wären. Laut einem Bericht von ZEIT ONLINE zumindest habe das Weiße Haus

> „ (…) zwar Bedenken geäußert, doch sei der Bundesregierung nicht untersagt worden, den Geheimdienstausschüssen des Bundestags die Liste zur Einsicht vorzulegen. Die letzte Entscheidung über eine Freigabe sei der Bundesregierung überlassen worden. Auch sei es eine „absolute Mär“, dass die US-Regierung mit einer Einschränkung der Geheimdienstkooperation gedroht habe, sollte die Liste öffentlich werden.“[78]

Vollends nicht nachvollziehbar ist die Entscheidung der Bundesregierung auch deshalb, weil Kanzleramtsminister Altmeier sich nach Auftauchen der NSA-Selektoren gegenüber den Parlamentsausschüssen in hohem Maße empört gezeigt und für die Bundesregierung eine öffentliche Erklärung mit heftiger Kritik am BND abgegeben hatte. Die Herausgabe der Selektorenliste an den Ausschuss schien danach nur eine Zeitfrage von zwei bis drei Wochen.

3. Drohungen gegenüber dem Ausschuss

Angesichts des öffentlichen Interesses an den Snowden-Enthüllungen vor allem in den Jahren 2013/14 ist es wenig verwunderlich, dass es aufgrund der Blockade-Haltung der Bundesregierung gegenüber der parlamentarischen Aufklärung zu einer Reihe von Leaks in der Presse kam.

---

78) *Zeit Online* vom 12. August 2015, „Kanzleramt darf Selektorenliste laut USA freigeben“, abrufbar unter http://www.zeit.de/digital/2015-08/nsa-affaere-weisse-haus-bundesregierung-selektorenliste.

In der Folge kündigte Kanzleramtsminister *Peter Altmaier* im im Oktober 2014 dem Ausschuss gegenüber Strafanzeigen an, sollte es zu weiteren Veröffentlichungen kommen, die sich auf eingstufte Unterlagen beziehen.[79]

Dabei bezog er sich explizit etwa auf Veröffentlichungen der *Süddeutschen Zeitung* zur Operation EIKONAL Anfang Oktober 2014 – die dem Ausschuss zum Zeitpunkt der Veröffentlichung gar nicht vollständig vorlagen. Zugang zu eingestuften Akten der Bundesregierung, die vom Untersuchungsausschuss beigezogen werden, haben neben den Mitgliedern des Ausschusses noch viele andere Personen aus Bundesregierung und der Bundestagsverwaltung. Ein Schreiben des Kanzleramts, das sich in einer solchen Angelegenheit nur an den Ausschuss richtet, muss folglich als Drohung verstanden werden. Die Oppositionsfraktionen weisen die damit insinuierten Vorwürfe zurück.

Im Februar 2015 kam es zu einem Vorfall, dass in der Presse beschrieben wurde als:

> „BND versucht NSA-Aufklärer in die Falle zu locken“[80]

In einer später als geheim eingestuft beschriebenen Obleute-Sitzung[81] berichteten Geheimdienst-Koordinator *Klaus-Dieter Fritsche* und der damaligen BND-Präsident *Gerhard Schindler* über ein Schreiben des britischen Nationalen Sicherheitsberaters *Paddy McGuinness*[82]. Der früh am nächsten Morgen über die Sitzung berichtende *Focus* wusste:

79 Ausschussdrucksache 245

80) *Süddeutsche Zeitung Online* vom 5. Februar 2015, „BND versucht NSA-Aufklärer in die Falle zu locken“, abrufbar unter http://www.sueddeutsche.de/politik/eklat-im-untersuchungsausschuss-bnd-versucht-nsa-aufklaerer-in-die-falle-zu-locken-1.2337559

81) Beratungsprotokoll-Nr. 34, S. 5

82) Beratungsprotokoll-Nr. 36, S. 6

> „Der britische Geheimdienst hat nach einem Bericht des Nachrichtenmagazins FOCUS der Bundesregierung mit dem Abbruch aller Kontakte zu deutschen Sicherheitsbehörden gedroht.“[83]

Tatsächlich berichtete Josef Hufelschulte für den Focus Details, die am Abend zuvor gar nicht genannt worden waren, weil die Obleute aller Fraktionen das Gespräch vor seinem Ende abbrachen. Grund war die Befürchtung, dem Ausschuss würden hoch eingestufte Details berichtet, die sich dann in der Presse wiederfänden, was der Bundesregierung als Anlass dienen könnte, Akten über gemeinsame Operationen deutscher und britischer Nachrichtendienste zurückzuhalten und zudem den Ausschuss für einen etwaigen Abbruch der Kooperation verantwortlich zu machen.[84]

4. Verhinderung der Aussage von Edward Snowden

Dass die Obstruktionspolitik der Bundesregierung und der Ausschussmehrheit in den vorgenannten Punkten von der Rechtsprechung des Bundesverfassungsgerichts und des Bundesgerichtshofes letztlich nicht beanstandet wurde, sollte (mag die Koalition dies auch als kurzfristigen Erfolg verbuchen) eigentlich auch für sie kein Grund für triumphalen Jubel sein. Denn dass die parlamentarische Kontrolle und damit das demokratische System hierdurch – als Kollateralschaden – geschwächt wurde, liegt auf der Hand. Die Oppositionsfraktionen im Ausschuss machen insoweit folgende kurze Bemerkungen auch zu Aspekten der genannten Rechtsprechung:

Zu Beginn der Legislaturperiode wurde im Deutschen Bundestag ein Konsens dahin erzielt, dass die Oppositionsfraktion auch aus demokratiepolitischen Gründen über ein Recht auf Einsetzung von Untersuchungsausschüssen verfügen sollten (§ 126a GO-BT). Dabei wurde auch vorgesehen, dass die Größe der jeweiligen Untersuchungsausschüsse so bemessen werden sollte, dass die Opposition im Ausschuss über – auch gerichtlich durchsetzbare – Minderheitenrechte verfügen sollte. Das Ergebnis der

83) Focus Online vom 5. Februar 2015, „Briten drohen mit Abbruch aller Kontakte zu Deutschland“, abrufbar unter http://www.focus.de/politik/deutschland/geheimdienst-eklat-briten-drohen-mit-abbruch-aller-kontakte-zu-deutschland_id_4454261.html.

84) *Golem.de* vom 5. Februar 2015, „NSA-Ausschuss empört über Drohungen des GCHQ“, abrufbar unter https://www.golem.de/news/kooperation-mit-bnd-nsa-ausschuss-empoert-ueber-drohungen-des-gchq-1502-112173.html.

o.g. Rechtsprechung ist nunmehr, dass diese Rechte einer Minderheit keinen Schutz durch den im PUAG vorgesehenen Rechtsweg zum BGH genießen. Denn dieser gilt entgegen des Wortlauts des PUAG laut BGH nur dann, wenn durch die Antragsteller „ein Viertel der Mitglieder der des Bundestages repräsentiert“ werden.[85] Durch den – hier gerichtlichen geführten – Kampf der Gegenseite gegen die Vernehmung des Zeugen Snowden ist also das demokratiepolitische Ziel beschädigt worden, dass auch die Regierungsfraktionen zu Beginn der Legislaturperiode noch für richtig gehalten hatten. Ergebnis ist also ein handfester Kollateralschaden für unsere – in Grundsatzfragen häufig noch konsensuale – Demokratie.

Mit dem gerade skizzierten Ergebnis ist auch ein wesentlicher Inhalt des PUAG verloren gegangen, auf den sich die Fraktionen des Deutschen Bundestages bei dessen Verabschiedung geeinigt hatten. Denn sogar der Prozessvertreter der Gegenseite im zitierten Verfahren ging bis zu den Rechtsstreitigkeiten im Falle Snowden davon aus, dass entsprechend dem Willen des Gesetzgebers „jedes situative Mitgliederviertel“ im Ausschuss ein „eigenständiges Antragsrecht“ habe.[86] Diese Auffassung war dabei ersichtlich auch deshalb die richtige, weil andernfalls auch die – grundsätzlich auch vom BVerfG betonte – Gleichheit aller Abgeordneten im Ausschuss nicht mehr gewahrt werden kann. Um es auch den Koalitionsfraktionen zu verdeutlichen: Auch zwei ihrer Abgeordneten aus unterschiedlichen Fraktionen können künftig derartige Anträge nicht mehr stellen, auch wenn jede dieser beiden Fraktionen über ein Viertel der Mitglieder des Bundestages verfügt und die beiden Abgeordneten ein Viertel der Mitglieder des Ausschusses bilden. Folgeschaden des Abwehrkampfes der Koalitionsfraktionen gegen eine sachgerechte Aufklärung durch Vernehmung des Zeugen Snowdens ist also auch die Durchbrechung des Grundsatzes der Gleichheit aller Abgeordneten im Ausschuss.

Wie schon oben angedeutet (siehe dort Behauptung der Zeuge sei Agent) ist im Übrigen Kollateralschaden des Verhaltens der Gegenseite in Sachen Vernehmung des

85) so BGH, Beschluss vom 23. Februar 2017, 3 ARs 20/16, Absatz-Nr. 19, http://juris.bundesgerichtshof.de/cgi-bin/rechtsprechung/document.py?Gericht=bgh&Art=en&nr=77709&pos=0&anz=1.

86) *Gärditz* in Waldhoff/Gärditz, PUAG, § 17, Rdnr. 32.

Zeugen Snowden die Wahrheit. Die Koalitionsfraktionen behaupten insoweit u.a. bis zum heutigen Tage, hier sei es nur um das „wie“ und nicht um das „ob“ der Vernehmung des Zeugen gegangen. Dies ist wie auch die Ermittlungsrichterin des BGH festgestellt hat, ersichtlich falsch.[87] Denn der Zeuge stand dem Ausschuss als solcher nur in Deutschland zur Verfügung. Um die Abgabe von allgemeinen Statements, wie sie Herr Snowden andernwärts gehalten hat, ging es bei einer Aussage des Zeugen vor dem Ausschuss von vorneherein nicht. Erforderlich gewesen wäre eine vertiefte Befragung des Zeugen. Dass der Zeuge diese nur unter dem Schutz des Landes durchführen wollte, das ein Interesse hatte (und hat), ihn vertieft zu befragen, versteht sich von selbst. Angesichts der schwierigen Einschätzung zur Lage in Russland haben die Oppositionsfraktionen insoweit volles Verständnis für die Haltung des Zeugen.

a) Die Feigheit der SPD

Die VertreterInnen der Mehrheit haben über drei Jahre einen beachtlichen Spagat vollbracht: der Zeuge Edward Snowden wurde direkt nach der Einsetzung des Ausschusses einstimmig beschlossen. Die restliche Zeit verbrachten sie gemeinsam mit der Bundesregierung damit, seine Ladung für eine Aussage vor dem Untersuchungsausschuss zu verhindern. Begleitet wurde dies durch die stetige Wiederholung, wie wichtig seine Aussage für den Ausschuss sei. Das Ganze gipfelt nun in der Unterstellung im Bewertungsteil der Mehrheit, die Opposition hätte die Aussage verhindert.

Die SPD hat sich dabei in besonderer Weise hervorgetan. Um nur ein – besonders illustratives – Beispiel zu nennen:

Im Oktober 2015 beantragte die Opposition, der Ausschuss möge die Konkretisierung der Ladung Edward Snowdens beschließen und darüber hinaus die Bundesregierung ersuchen, unverzüglich die Voraussetzungen für seine Vernehmung in Deutschland zu schaffen.

87) Beschluss vom 11. November 2016 (1 ARs 1/16; Absatz-Nr. 33), http://www.hrr-strafrecht.de/hrr/1/16/1-bgs-125-16.php.

In der Beratungssitzung am 15. Oktober beantragte die SPD, den zweiten Teil des Antrags der Opposition zu vertagen – den ersten lehnte die Mehrheit sofort ab.[88].

Erst zwei Tage vorher hatte die SPD Sarah Harrison den Internationalen Willy-Brandt-Preis verliehen:

> „Sie hat mit ihrem Engagement für WikiLeaks und speziell durch ihre journalistische Begleitung von Edward Snowden großen politischen Mut bewiesen. Ihr Wirken steht exemplarisch für das Streben nach Transparenz und den Einsatz gegen ausufernde Überwachung."[89]

In der folgenden Beratungssitzung am 5. November 2015 lehnte die Mehrheit dann auch den zweiten Teil des Antrags der Opposition ab[90], nur um sodann einen eigenen Antrag auf Vernehmung Edward Snowdens in Moskau zu beschließen, die per Video-Übertragung vorgenommen werden sollte, wobei ihr bekannt war, dass Snowden dies bereits abgelehnt hatte Der Antrag endet mit den Worten:

> „Dem Zeugen wird zudem mitgeteilt, dass er auf seinen Wunsch hin an diesem oder einem anderen Termin alternativ auch nicht förmlich als sonstige Auskunftsperson oder als Sachverständiger an seinem gegenwärtigen Aufenthaltsort oder andernorts außerhalb Deutschlands gehört werden könnte." [91].

Dies mutete auch deswegen zynisch an, weil das Europäische Parlament seine Mitgliedsstaaten genau eine Woche zuvor aufgerufen hatte,

> „etwaige Strafanzeigen gegen Edward Snowden fallenzulassen, ihm in Anerkennung seines Status als Informant und international tätiger

---

88) Beratungsprotokoll-Nr. 66, S. 4 f.

89) Pressemitteilung der SPD „Verleihung des 4. Internationalen Willy-Brandt-Preises an die ungarische Philosophin Àgnes Heller und die britische Journalistin Sarah Harrison" vom 13. Oktober 2015, abrufbar unter https://www.spd.de/presse/pressemitteilungen/detail/news/verleihung-des-4-internationalen-willy-brandt-preises-an-die-ungarische-philosophin-agnes-heller-und-die-britische-journalistin-sarah-harrison/13/10/2015/.

90) Beratungsprotokoll-Nr. 68, S. 6.

91) Ausschussdrucksache 435.

> Menschenrechtsverfechter Schutz zu gewähren und folglich seine Ausweisung und Auslieferung durch Dritte zu verhindern“[92]

b) Verschleppung durch vage Antworten der BReg an UA und Untätigkeit bei der Prüfung der Strafvorwürfe gegen Snowden insb. im BMJV

Eine besonders unrühmliche Rolle bei der Verhinderung der Aussage von Edward Snowden spielte das Bundesjustizministerium (BMJV).

Zwischen November 2014 und Februar 2017 wurde das BMJV vom gesamten Ausschuss oder einzelnen Abgeordneten in regelmäßigen Abständen gefragt, ob der Bundesregierung inzwischen bekannt sei, was Snowden in den USA vorgeworfen werde und ob die Bundesregierung also entschieden habe, ob ihm in der Konsequenz in Deutschland Auslieferungsschutz wegen politischer Verfolgung in den USA gewährt werden würde.

Die Beratungen der einzelnen Fragen dauerten jeweils Monate. So wurde der Vertreter des BMJV etwa im November 2015 gefragt, ob es zum Auslieferungsschutz eine Entscheidung gebe, eine Woche später wurde seitens des BMJV mitgeteilt, dass eine Beratung mit dem Auswärtigen Amt (AA) erforderlich sei. Einen Monat später hatte die Ressortbesprechung mit dem Ergebnis stattgefunden, dass ein Fragenkatalog an die US-Regierung geschickt werden sollte. Anfang Juni 2016, also fünf Monate später, teilte das BMJV dem Ausschuss mit, dass der Fragenkatalog nun verschickt worden sei. Im Oktober 2016 wurde in der Fragestunde des Bundestages eine weitere Ressortabstimm angekündigt. Bis zum Ende der Beweisaufnahme im Februar 2017 konnte die Bundesregierung jedoch keine Angaben dazu machen, wie sich diese Ressortabstimmung entwickelt hatte.[93]

---

92) Entschließung des Europäischen Parlaments vom 29. Oktober 2015 zur Weiterbehandlung der Entschließung des Europäischen Parlaments vom 12. März 2014 zur elektronischen Massenüberwachung der Unionsbürger (2015/2635(RSP)).

93) Beratungsprotokoll-Nr. 19, S. 4, Nr. 29, S. 5, Nr. 68, S. 4 f., Nr. 71, S. 7 f., Nr. 127, S. 7, Nr. 129, S. 6, außerdem Ausschussdrucksachen 248, 262, 451 und 492.

Dieses Verhalten des Justizministeriums ist in höchstem Maße zynisch angesichts der Situation Snowdens, der in Moskau den Launen der russischen Regierung unterworfen ist, während ihm den USA wahrscheinlich jahrzehntelanger Haft droht.

IV. Massenüberwachung

Die Mehrheit des Ausschusses hat in den Untersuchungen das Ziel verfolgt festzustellen, dass es keine unzulässige anlasslose Massenüberwachung gebe – vor allem nicht von Deutschen oder auf deutschem Boden, weder durch die *Five Eyes* noch durch die deutschen Geheimdienste. Einige der Abgeordneten haben bei jeder passenden oder auch nicht passenden Gelegenheit nach Zeugenaussagen triumphierend verkündet, dass eine Massenüberwachung nicht bestätigt wurde. Keine anlasslose Massenüberwachung konnte festgestellt werden, steht auch in der abschließenden Bewertung durch die Mehrheit.[94]

Doch das stimmt nicht. Das Ergebnis der Beweisaufnahme war ein anderes.

Dass deutsche und andere Nachrichtendienste massenhaft und anlasslos Kommunikationddaten erfasst und auswertet, haben die Ergebnisse der Untersuchung klar gezeigt.

1. Massenüberwachung Deutscher in Deutschland

In den veröffentlichten Dokumenten aus dem Besitz von *Edward J. Snowden*, die dem Ausschuss vorlagen, finden sich zahlreiche Belege für anlasslose Massenüberwachung durch die NSA, von denen Bundesbürger_innen ebenfalls betroffen und deutsche Dienste beteiligt waren. Offen geblieben ist, wo die Daten abgegriffen wurden – direkt in Deutschland oder im Ausland. Deutlich wird aber, dass die Spionage zumindest auch an Glasfaserknotenpunkten, wie etwa in Südengland bei Bude bzw. vor der englischen Südküste stattfindet. Der britische Geheimdienst GCHQ hatte im Rahmen von TEMPORA neben zahlreichen weiteren Glasfaserleitungen unter anderem Zugriff auf das Überseekabel TAT-14. Hierüber liefen auch deutsche Telekommunikationsdaten.[95]

---

94) Mehrheitsbewertung, S. 32 (Fassung vom 28.4.2017).

95) *Süddeutsche Zeitung* vom 28.08.2013 „Britischer Geheimdienst zapft Daten aus Deutschland an“, http://www.sueddeutsche.de/politik/internet-ueberwachung-britischer-geheimdienst-zapft-daten-aus-deutschland-ab-1.1757068, abgerufen am 16. Juni 2017.

Zudem werden Daten in großem Umfang in den USA bei dortigen Servern abgegriffen. Massendaten wurden hier von großen IT-Unternehmen wie *Microsoft, Google, Yahoo*, *Facebook* oder *Apple* direkt der NSA zur Verfügung gestellt.[96] Da immer mehr Telekommunikation von Deutschen aus Deutschland nicht nur ins Ausland über Glasfaserleitungen und Knoten über die USA geleitet wird, sondern gerade auch Verkehre über den „Umweg“ USA von Deutschland nach Deutschland bewegt werden, ist es wahrscheinlich, dass auch letztere diese unterwegs auf diesen Wegen abgegriffen und ausgespäht werden.

Die eigentlich notwendige nähere Aufklärung dieser Ausspähoperationen konnte der Untersuchungsausschuss nicht vornehmen, weil die dafür unverzichtbaren Akten und Unterlagen aus den USA bzw. Großbritannien genauso wenig zur Verfügung standen, wie Zeug_innen aus diesen Ländern. In den von der Bundesregierung dem Ausschuss vorgelegten Unterlagen fanden sich dazu keine Beweise. Ob gleichwohl beim BND oder bei der Bundesregierung dazu Kenntnisse oder Unterlagen vorhanden sind, konnte der Ausschuss schon deshalb nicht klären, weil die vorliegenden Akten, wie erwähnt, aus unterschiedlichen Beständen von BND und Bundeskanzleramt nach deren Ermessen zusammengestellt worden sind und ihnen keineswegs alles Vorhandene lesbar zu entnehmen ist.

Die Dokumente aus dem Besitz von *Snowden* sind durchaus beweisgeeignet. Im Sommer 2013 wurde zwar von Mitarbeiter_innen der deutschen Geheimdienste und des Kanzleramts immer wieder in Frage gestellt, ob diese Dokumente authentisch sind nach dem Motto: Es handele sich ja nur um Kopien, die jede/r X-Beliebige anfertigen könne. Originale würden ja nicht vorgelegt. Aber inzwischen zweifelt niemand, der ernstgenommen werden will noch daran, dass es sich um authentische Ausdrucke aus den Datenbeständen der NSA handelt. Auch von Seiten der Leitungsebenen amerikanischer Geheimdienste wurde nicht bestritten, dass die Dokumente authentisch sind. Sonst hätte es ihren Ärger und ihre Unmutsäußerungen auch nicht gegeben. Sie hätten *Snowden* nicht des Verrats und zahlreicher Verbrechen bezichtigt. Lediglich über die Interpretation einzelner Dokumente oder von deren Teilen durch Journalist_innen

---

96) Snowden-Dokument, Powerpoint zu PRISM, MAT A Sek-1c, Bl. 42 (45).

gibt es Streit und unterschiedliche Auffassungen. Soweit ersichtlich, wird die Echtheit der Dokumente von der Mehrheit des Ausschusses nicht bezweifelt und nicht in Frage gestellt.

Etwa verbliebene Zweifel an der Echtheit der Dokumente hätten die Mitglieder des PUA beseitigen können, indem sie *Snowden* als Zeuge vor dem Ausschuss in Berlin gehört hätten. Der Zeuge hätte unter Wahrheitspflicht dazu vernommen werden können, wie und woher er die Dokumente beschafft hatte. Er war dazu bereit. Der von ihm bevollmächtigte Rechtsanwalt *Kaleck*, hat dies dem Ausschuss auch schriftlich mitgeteilt. *Snowden* hätte als langjähriger Mitarbeiter der US-Geheimdienste auch fachkundige Auskünfte für die Feststellung der Authentizität und Interpretation der Dokumente geben können.

Näher befassen konnte sich der Ausschuss nur mit den Ausspähoperationen in Deutschland, zu denen ihm Akten und Zeug_innen zur Verfügung standen.

2. Massenüberwachung durch die Operation EIKONAL auch von Deutschen

Anlasslose Massenüberwachung in gigantischem Ausmaß hat die Beweisaufnahme z.B. bei der Operation EIKONAL festgestellt[97]. Datenströme aus der Satteliten- und Glasfasererfassung wurden ausspioniert. Über Glasfaserkabel geleitete Paketverkehre spielten eine immer größere Rolle, wegen der Vorteile viel größerer Datenmengen und der schnelleren Weiterleitung. Der Heuhaufen an Daten, der ausgespäht und überwacht wurde und wird, ist unermesslich groß. Die ständigen Metadatenströme wurden mit hundertausenden Selektoren durchsucht, Treffer ausgeleitet und an die NSA weitergeben. Datenverkehre auf Strecken von Ausland zu Ausland über Glasfaserkabel waren uneingeschränkt Objekte der Ausspähung bzw. „zum Abschuß freigegeben“[98] wie ein Zeuge aus dem BND es in der Ausschussbefragung formulierte. Eine Teilmenge von 20 Prozent auszuspähen wie vielleicht bei Satellitenverkehren reichte dem BND nicht. Etwaig doch erfasste „G 10-geschützte“ Daten sollten ausgeleitet und

97) Vgl. hierzu das nachfolgende Kapitel V – Kooperation des BND mit der NSA: EIKONAL und Bad Aibling.

98) *T. B.*, Protokoll-Nr. 20, S. 44.

gelöscht werden. Aber es stellte sich heraus, dass dies zu hundert Prozent nicht möglich war. Im BND war das bekannt. Mitarbeiter_innen befürchteten das öffentliche Bekanntwerden dieser Praxis. Doch die Operation wurde gleichwohl fortgesetzt und damit auch die rechtswidrige anlasslose Massenüberwachung. Dabei war aber nicht nur die Überwachung der Daten von, nach BND-Meinung „G 10-geschützten" Rechtsträger_innen, also von Deutschen, unzulässig und auszufiltern. Ein Abschätzen der Zahl der von der rechtswidrigen Überwachung Betroffenen war nach Angaben der Zeug_innen aus dem BND nicht möglich oder abschätzbar. Der Ausschuss war selbst nicht in der Lage, diese Zahlen näher zu ermitteln. Aber schon die kolportierten Zahlen an die NSA monatlich ausgeleiteter Datensätze lassen keinen Zweifel zu, dass es sich um eine unüberschaubare Masse Betroffener geht.

3. Massenüberwachung mittels der NSA-Selektoren

40 000 Selektoren, die NSA dem BND mit der Bitte um Einsteuerung zum Ausspähen übermittelt hatte, hatten Mitarbeiter_innen des BND im Auguste 2013 wohl unter dem Eindruck der Veröffentlichung der Dokumente *Snowdens* – die seit zwei Monaten andauerte – bei Überprüfung als unzulässig ausgesondert. Es handelte sich um eine Teilmenge der mehreren hunderttausend Selektoren, die von der NSA zum Zweck des Ausspionierens an den BND geleitet hatte. Im BND wurden diese Selektoren vor der Einsteuerung nicht überprüft. Das wäre gar nicht möglich gewesen. Konkrete Anlässe, Gründe und Hintergründe für die Einsteuerung wurden dem BND nämlich gar nicht mitgeteilt. Die NSA-Selektoren konnte der Ausschuss nicht aufklären, weil sie im Kanzleramt unter Verschluss gehalten und dem Ausschuss grundlos und beharrlich verweigert wurden. Auch inwieweit mit den Suchbegriffen Treffer erzielt wurden, konnte nicht festgestellt werden, genauso wenig, was an die NSA davon weitergeleitet wurde. Jedenfalls waren diese Selektoren und ihre Einsteuerung unzulässig auch nach Meinung des BND, sonst hätte er sie nicht aus der Steuerung herausgenommen und dies der NSA mitgeteilt. Nach Einschätzung der „Vertrauensperson" der Bundesregierung *Graulich* waren sie überwiegend rechtswidrig und die Einsteuerung ein großer Fehler des BND. Ca. 40 000 NSA-Selektoren wurden ausgesteuert, aber welche weiteren aus der Masse der Hundertausenden NSA-Selektoren vielleicht ebenfalls unzulässig waren, konnte der Ausschuss nicht beurteilen, weil er sie nicht prüfen konnte. Auch diese

wurden von der Bundesregierung nicht zur Verfügung gestellt. Ob deutsche Grundrechtsträger_innen betroffen waren, muss aus den genannten Gründen offenbleiben.

4. Massendatenüberwachung mittels BND-Selektoren

Auch mehr als 3000 eigene Selektoren hat der BND Anfang August 2013 aus der Steuerung herausgenommen, weil sie zwar nicht anlasslos zum Ausspähen genutzt wurden, aber aus unzulässigem Anlass, etwa weil befreundete EU-Regierungen, EU-Institutionen und NATO-Partner damit ausspioniert wurden. Auch deutsche Staatsbürger_innen waren unter den Überwachten, wie den Überwachungsergebnissen zu entnehmen war, und zwar unter dem Vorwand, sie stünden als „Funktionsträger_innen" von nichtdeutschen Unternehmen nicht mehr unter dem Schutz des Artikel 10 GG, sondern seien wie Ausländer zu behandeln. Die gesamte Einsteuerung dieser bemakelten BND-Selektoren war nach deutschem, aber auch nach EU-Recht rechtswidrig. Zum Teil verstieß sie gegen Art. 10 GG. Die konkrete Überprüfung der BND-Selektoren, ihrer Anlässe und Ergebnisse, war dem Untersuchungsausschuss nur in wenigen Einzelfällen möglich, weil darüber hinaus die Unterlagen dafür nicht mehr zur Verfügung standen oder nicht vorgelegt wurden. Ende Oktober 2013 erging, einen Tag nach der öffentlichen Äußerung der Kanzlerin: „Ausspähen unter Freunden, das geht gar nicht"[99] die Anweisung des Kanzleramts in den BND, die Einsteuerung solcher Selektoren sofort zu stoppen. Nicht zuletzt auch daraus folgt, dass nicht ausreichend zulässige Anlässe für solche Überwachung bestanden. Es handelte sich um anlasslose Massenüberwachung. Die Einsteuerung solcher BND-Selektoren wurde ab Frühjahr 2014 trotzdem für Teilbereiche wieder aufgenommen.

5. Inhalt und Auswirkungen anlassloser massenhafter Überwachung

Der Untersuchungsauftrag enthält weder den Begriff *Massenüberwachung* noch die Formulierung *anlasslos*. Der Begriff *anlasslose Massenüberwachung* wurde insbesondere durch die Enthüllungen *Edward J. Snowdens* geprägt, als in deren Folge das

99) Pressestatement von Bundeskanzlerin *Merkel* vor der Sitzung des Europäischen Rates am 24. Oktober 2013, https://www.bundesregierung.de/ContentArchiv/DE/Archiv17/Mitschrift/Pressekonferenzen/2013/10/2013-10-24-merkel-er.html, abgerufen am 15. Juni 2017.

tatsächliche Ausmaß weltweiter Überwachung durch die Nachrichtendienste der *Five Eyes* deutlich wurde: Über Jahre und unter Umgehung der Öffentlichkeit und teilweise auch der Parlamente haben Geheimdienste in unterschiedlich intensiver Kooperation und Zusammenarbeit eine gigantische digitale Überwachungsinfrastruktur errichtet. Frei nach den NSA-Zielen „Collect it All“, „Process it All“, „Sniff it All“, „Partner it All“, „Exploit it All“ und „Know it All”[100] betreiben sie hunderte zusammenwirkende Programme, mit dem Ziel, jederzeit auf sämtliche verfügbaren Daten jedes Einzelnen weltweit zugreifen zu können. Diese besondere Qualität der Überwachungsinfrastruktur, insbesondere die Quantität und Intensität flächendeckender nachrichtendienstlicher Telekommunikationsüberwachung, findet ihren Ausdruck im Begriff Massenüberwachung. Wurde zunächst die US-Debatte umfänglich unter diesem Oberbegriff Mass Surveillance geführt,[101] so hat er unlängst auch in die bundesdeutsche Auseinandersetzung über geheimdienstliche Überwachung Einzug gehalten. Hier gilt er bislang nicht als feststehender Rechtsbegriff, sondern dient vielmehr als Bezugs- und Ausgangspunkt elementarer grundrechtlicher Kernfragen. Die verfassungsrechtliche Beschäftigung reicht dabei bereits lange zurück.[102] Die Bedeutung erwächst heute insbesondere mit Blick auf die Erkenntnisse des Untersuchungsausschusses, die die Vermutung stützen, dass der BND nicht nur Teil der weltweiten geheimdienstlichen Kooperationen ist, sondern bereits unter Mithilfe der NSA eine vergleichbare Überwachungsinfrastruktur unter bundesdeutscher Führung errichtet hat. Die Menschen in der Bundesrepublik sind somit längst nicht mehr nur massenhaft von Maßnahmen der *Five Eyes* betroffen, sondern erfahren auch Grundrechtsverletzungen durch anlasslose, massenhafte Überwachungen durch die deutschen Nachrichtendienste.[103]

---

100) *Glenn Greenwald*, No Place To Hide, S. 97, NSA-Folie „New Collection Posture”; *David Cole*, ‘No Place to Hide’ by Glenn Greenwald, on the NSA’s sweeping efforts to ‘Know it All’, The Washington Post vom 12. Mai 2014 https://www.washingtonpost.com/opinions/no-place-to-hide-by-glenn-greenwald-on-the-nsas-sweeping-efforts-to-know-it-all/2014/05/12/dfa45dee-d628-11e3-8a78-8fe50322a72c_story.html, abgerufen am 12. Juni 2017.

101) *Margaret Hu,* Taxonomy of the Snowden Disclosures, S. 1681 f., 72 Wash. & Lee L. Rev. 1679 (2015), http://scholarlycommons.law.wlu.edu/wlulr/vol72/iss4/4, abgerufen am 12. Juni 2017.

102) BVerfGE 65, 1-71, Rn. 176 (Volkszählungsurteil), abrufbar unter https://openjur.de/u/268440.html.

103) Vgl. insbesondere Kapitel V.9 – Datenübermittlungen des BND an die NSA aus Bad Aibling.

a) Die Überwachung ist massenhaft

Massenüberwachung folgt dem Ziel der Ermöglichung vollständiger geheimdienstlicher Erfassung und Auswertung von Telekommunikation und Internetverkehr weltweit. Sie wird durch die Struktur und Funktionsweise der digitalen Kommunikation ermöglicht. Dass schlicht alle Nutzer_innen moderner Kommunikationssysteme von der einzelfallunabhängigen Überwachung betroffen sind, ergibt sich bereits aus dem „Collect it All“-Ansatz. Die massenhafte Betroffenheit auch der bundesdeutschen Bevölkerung beruht dabei auf den vielfältigen Gelegenheiten möglicher Erfassung und Speicherung der persönlichen Kommunikationen, Daten und Informationen.[104] Dies geschieht unmittelbar durch geheimdienstliche Abgriffe (TEMPORA, UPSTREAM oder XKEYSCORE) oder durch geheimdienstliche Zugriffe bei privaten Providern und Plattformanbietern (PRISM). Bei den anschließenden Rasterzugriffen kann mittels unterschiedlichster Selektorverfahren und maschineller Analyseverfahren in eine enorme Tiefe von Kommunikationsebenen vorgedrungen werden, sodass die Darstellung ganzer Beziehungsgeflechte von Personen möglich wird. Nicht zuletzt wird hierdurch aus wirtschaftsinformatischer Sicht ein Fokus auf Big Data, Big Data-Auswertungen und somit Wirtschaftsspionage in großem Stil ermöglicht.

Aufgrund der Funktionsweise paketvermittelter Kommunikation ist eine Ausfilterung von personenbezogenen Daten unbescholtener Personen bei den unterschiedlichen Verfahren allenfalls in geringem Umfang möglich. Damit werden millionenfach Meta- und Inhaltsdaten auch von Bundesbürger_innen tagtäglich zum Gegenstand von Abgriffen, Speicherung, Rasterung, Selektion, maschineller Analyse und Datenweitergabe. Auch der ehemalige Bundesbeauftragte für den Datenschutz und die Informationsfreiheit *Peter Schaar* erklärte vor dem Untersuchungsausschuss, dass zur Massendatenerfassung

> „der gesamte Prozess der Erfassung [gehört], das heißt einschließlich der Datenerhebung. Und insofern ist das, was zum Beispiel im Bereich

104) *Margaret Hu*, Taxonomy of the Snowden Disclosures, S. 1690, 72 Wash. & Lee L. Rev. 1679 (2015), http://scholarlycommons.law.wlu.edu/wlulr/vol72/iss4/4, abgerufen am 12. Juni 2017.

> der strategischen Fernmeldekontrolle stattfindet, schon eine Form von Massendatenverarbeitung oder Massendatenerfassung. Das, was bei der Vorratsdatenspeicherung bei uns stattgefunden hat oder in den USA oder Frankreich nach wie vor stattfindet, ist auch eine Form von Massendatenerfassung.“[105]

b) Die Überwachung ist anlasslos

Massenüberwachung erfolgt ohne konkreten Anlass.[106] Anders als herkömmliche Telekommunikationsüberwachung setzt sie gerade nicht an einem konkreten Verdachtsmoment, einer spezifischen Gefahrensituation oder gezielt an der Kommunikation einer, aus behördlicher Sicht verdächtigen Person an. Bei anlasslosen Ausleitungs-, Analyse-, oder Rasterverfahren von Mobilfunk- oder Internetverkehren wird vielmehr ganzheitlich an der Infrastruktur selbst angesetzt. Da mit dem Anlass auch die hierin festgelegte zeitliche oder räumliche Begrenzung der Maßnahme entfällt, liegt die vage Grenze der Überwachung lediglich noch im mit ihr verfolgten Erkenntnisziel selbst. Auch eine allgemeine Bedrohungslage erscheint als zu wenig konturiert, um als Anlass noch gelten zu können.[107]

Verheerend ist in diesem Zusammenhang, dass Personen, die sich anonym im Internet verhalten, besonders häufig von Maßnahmen durch die Geheimdienste betroffen sind. Denn auf der Suche nach bislang unbekannten Verdächtigen werden Datenströme nach „abweichenden Ereignissen“ durchforstet. Neben Anhaltspunkten wie einer auffälligen Sprache, also einer Sprache, die an einem bestimmten Aufenthaltsort

---

105) *Schaar*, Protokoll-Nr. 31 I, S. 24.

106) Der Begriff „anlasslos“ stammt aus der polizeirechtlichen Debatte und markiert Verfahren wie die Schleierfahndung oder Videoüberwachung.

107) *Bäcker*, Strategische Telekommunikationsüberwachung auf dem Prüfstand, K&R 2014, 556-561 (556); *Bäcker*, Verfassungsbeschwerde (Artikel-10-Gesetz), S. 5, https://freiheitsrechte.org/home/wp-content/uploads/2016/10/GFF-AI-G10-Verfassungsbeschwerde-anonymisiert.pdf, abgerufen am 12. Juni 2017.

als deplatziert erscheint, oder verdächtigen Inhalten, sind dies vor allem Verwendungen von Anonymisierungs- und Verschlüsselungstechnologien.[108]

So stellt beispielsweise die Decodierung (das Lesbarmachen von Inhalten) eine der zentralen Funktionen der Spähsoftware XKEYSCORE dar – einer Software, die auch die deutschen Nachrichtendienste BND und BfV in unterschiedlicher Weise verwenden[109] . Ein Blick hinter den Quellcode dieser amerikanischen Software, lässt erkennen, dass Nutzer_innen automatisch als Extremist_innen markiert werden, wenn sie im Internet nach Anonymisierungs-Tools wie *Tor* oder *Tails* suchen. So erging es beispielsweise dem deutschen Studenten *Sebastian Hahn*. Er entdeckte die IP-Adresse einer seiner Server im Quellcode von XKEYSCORE wieder. Weil er einen Server für das Anonymisierungsnetzwerk *Tor* betrieb, wurde er zum gezielten Objekt geheimdienstlicher Überwachungsmaßnahmen. Dass dies zugleich auch für sämtliche Nutzer_innen gilt, die auf seinen Server ebenfalls zugriffen, kann nicht ausgeschlossen werden.[110]

Vor diesem Hintergrund liest sich die leitende Antwort der Bundesregierung auf den NSA-Skandal – Bürger_innen müssten sich im Internet selbst schützen – wie ein Hohn, wenn doch explizit gerade auch diejenigen, die um die Sicherheit ihrer Daten besorgt sind und Verschlüsselungen verwenden, gerade deshalb zum Ziel von Überwachungen werden.

c) Die allgemeine Möglichkeit, von Überwachung betroffen zu sein

Entscheidend ist, die aufgrund der errichteten Überwachungsinfrastruktur gegebene Möglichkeit gezielter Erfassung oder auch flächendeckender Beobachtung ganzer Bevölkerungen – jederzeit und ohne großen Aufwand. Der Begriff Massenüberwachung ist dadurch charakterisiert, hinnehmen zu müssen, dass die eigenen Daten allein für

---

108) Vgl. *Lischka* und *Stöcker*, „NSA-System XKeyscore – Die Infrastruktur der totalen Überwachung“, Spiegel Online vom 31.07.2013, 21:00 Uhr, abgerufen am 12.Juni 2017.

109) Vgl. hierzu Kapitel VII Nutzung von XKEYSCORE durch BND und BfV.

110) *Kampf, Goetz* und *Kabisch*, „Quellcode entschlüsselt: Beweis für NSA-Spionage in Deutschland“, NDR.de vom 03.07.2014, http://www.ndr.de/nachrichten/investigation/Quellcode-entschluesselt-Beweis-fuer-NSA-Spionage-in-Deutschland,nsa224.html, abgerufen am 12. Juni 2017.

geheimdienstliche Zwecke erfasst, gespeichert, indiziert, durchsucht, mitgerastert und maschinell analysiert werden. Dabei werden in unvorhersehbarer Weise tiefste Einblicke in das Privatleben genommen. Die Überwacher holen weder eine Zustimmung der Einzelnen ein, noch benachrichtigen sie die Betroffenen nachträglich. Ein Rückgriff auf persönliche Daten wird damit für die Betroffenen weder unmittelbar spürbar noch ersichtlich. Sie verbleiben in der Ungewissheit, auch wenn sie selbst womöglich nie zum konkreten Objekt gezielter Überwachung werden. Dies bringt gleichwohl zwei Folgen mit sich: Zum einen können Betroffene zumindest nur plausibel annehmen, Überwachungsmaßnahmen ausgesetzt zu sein. Einen konkreten, substantiierten Nachweis der eigenen Betroffenheit durch unrechtmäßige, behördliche Datenerhebung und anschließende Verwendung zu erbringen, ist ihnen aufgrund der Heimlichkeit der Maßnahmen so gut wie nie möglich. Damit bleibt ihnen die Geltendmachung etwaiger Folgerechte auf Löschung, Berichtigung oder Genugtuung grundsätzlich verwehrt.[111]

Des Weiteren bringt der Möglichkeitsaspekt im Zusammenhang mit fehlender, angemessener Transparenz und mangelnder Kontrollierbarkeit von Massenüberwachung eine weitere erhebliche Gefahr mit sich: Die Gefahr der Selbstzensur. Sie ist Resultat des stetigen Generalverdachts, der diffusen Unkenntnis, gepaart mit einem Wissen über die potentielle Möglichkeit staatlichen Überwachtwerdens – auch in höchstpersönlichen Lebensbereichen. Das Bundesverfassungsgericht (BVerfG) warnte in seiner Entscheidung zur Vorratsdatenspeicherung vor eben jenem „Gefühl des unkontrollierbaren Beobachtetwerdens“, das durch die anlasslose, massenhafte Datenspeicherung „in besonderer Weise“ befördert wird.[112] Denn die Massenüberwachung bringt als staatliches Handeln mittelbar einschüchternde, abschreckende Effekte hervor, die die Bürger_innen davon abhalten, von ihren Freiheitsrechten Gebrauch zu machen. So betrifft Überwachung nicht nur die jeweils durch einen konkreten, individuellen Grundrechtseingriff verletzte Person, sondern hat permanente, mittelbare Auswirkungen auf

111) Vgl. BVerwG, Urteil vom 28. Mai 2014 – 6 A 1/13 –, BVerwG149, 359-373 http://www.bverwg.de/entscheidungen/entscheidung.php?ent=280514U6A1.13.0, abgerufen am 16. Juni 2017; BVerfG, Beschluss des Zweiten Senats vom 20. September 2016 – 2 BvE 5/15 –, http://www.bverfg.de/e/es20160920_2bve000515.html , abgerufen am 13.Juni 2017.

112) BVerfG, Urteil vom 2. März 2010 – 1 BvR 256/08, BVerfGE 125, 260 (323), http://www.bverfg.de/e/rs20100302_1bvr025608.html, abgerufen am 13. Juni 2017.

die Gesellschaft als Ganzes und ihr Gemeinwohl.[113] Bei diesen sogenannten *Chilling Effects* handelt es sich um eine in der Rechtsprechung des BVerfG und des Europäischen Gerichtshof für Menschenrechte (EGMR) seit langem anerkannte Rechtsfigur, die den Grundrechten damit einen objektivrechtlichen Schutzgehalt zuspricht. So hob das BVerfG bereits im Jahr 1983 in seinem Volkszählungsurteil hervor:

> „Individuelle Selbstbestimmung setzt (…) – auch unter den Bedingungen moderner Informationsverarbeitungstechnologien –voraus, daß dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten. (…) Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. **Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen**."[114]

Das Resultat: Anlasslose Massenüberwachung beeinträchtigt nachhaltig die unbefangene Wahrnehmung der Freiheitsrechte jeder/s Einzelnen. Eine Totalerfassung der Telekommunikation steht jedoch, das betont das BVerfG selbst, im Widerspruch zur verfassungsrechtlichen Identität der Bundesrepublik.[115]

---

113) *Assion*, Überwachung und Recht, Telemedicus-Schriftenreihe Bd. 1, Sommerkonferenz 2014, S. 33ff. https://www.telemedicus.info/uploads/Dokumente/Ueberwachung-und-Recht-Tagungsband-Soko14.pdf, abgerufen am 12.Juni 2017; *Cornelius*, Strafrechtliche Verantwortlichkeiten bei der Strategischen Telekommunikationsüberwachung, JuristenZeitung 2015, 693 (694).

114) BVerfG, Urteil vom 15. Dezember 1983 – 1 BvR 209/83 –, BVerfGE 65, 1-71 (mit eigenen Hervorhebungen); vgl. BVerfG, Beschluss vom 17. Februar 2009 (Az. 1 BvR 2492/08) Rn. 122f., abrufbar unter https://www.bverfg.de/e/rs20090217_1bvr249208.html.

115) BVerfG, Urteil vom 2. März 2010 – 1 BvR 256/08, BVerfGE 125, 260, 324, https://www.bverfg.de/e/rs20100302_1bvr025608.html.

d) Anlasslose Massenüberwachung ist verfassungswidrig

Die massenhafte, anlasslose Überwachung personenbezogener Daten ist nie verhältnismäßig und damit stets verfassungswidrig. Sie stellt einen erheblichen Eingriff in individuelle und extraterritorial für alle Menschen gleichermaßen geltende Freiheitsrechte dar – insbesondere in das Fernmeldegeheimnis und den Kernbereich der Telekommunikationsfreiheit gemäß Art. 10 GG[116] sowie das Recht auf informationelle Selbstbestimmung dar. Jede einzelne Erhebung, Verarbeitung und Nutzung eines personenpezogenen Datums stellt nach der Rechtsprechungd es BVerfG einen Grundrechtseingriff dar, der eigenständig zu bewerten ist, und besitzt datenschutzrechtliche Relevanz.

Dem Schutz des Fernmeldegeheimnisses unterfallen dabei sowohl die Inhalte der verschiedenen Kommunikationsformen als auch sämtliche äußeren Umstände der Kommunikation, die Auskunft über Ort, Gesprächsteilnehmer_innen, Dauer der Unterhaltung etc. geben.

Die Wahrnehmung des Rechts auf informationelle Selbstbestimmung bleibt dabei ebenso verwehrt wie das Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme in Fällen, bei denen das Endgerät von Bürger_innen betroffen ist bzw. infiltriert wird. In Folge der *Chilling Effects* setzt in zunehmendem Maße eine Bedrohung der freien, ungehinderten Kommunikation zwischen Menschen und des Rechts auf freie Meinungsäußerung ein.

Anlasslose Massenüberwachung hat enorme negative Auswirkungen auf das Zusammenleben und Wirken einer freiheitlichen demokratischen Zivilgesellschaft.[117] Mit ihr geht ein mit der Rechtsordnung unvereinbarer Generalverdacht gegen alle Bürger_innen einher. Sie widerspricht den Grundsätzen der Menschenwürde, der Privatheit von Kommunikation, der Persönlichkeitsrechte und datenschutzrechtlichen Prinzipien wie

116) Sachverständigengutachten von *Bäcker*, MAT A SV-2/3, S. 14; *Hoffmann-Riem*, MAT A SV-2/1, S. 11; *Papier*, MAT A SV-2/2, S. 7.

117) *Navi Pillay*, mass surveillance violates human rights, statement of the UN High Commissioner for Human Rights on Human Rights Day 10. Dezember 2013 http://www.unric.org/en/latest-un-buzz/28900-pillay-mass-surveillance-violates-human-rights, abgerufen am 12. Juni 2017.

der Datenvermeidung bzw. -sparsamkeit und Zweckbindung. Die zum Schutz freier und unüberwachter Kommunikation in der Demokratie eigens geschaffenen Grundrechtsgewährleistungen werden durch unbegrenzte Datenabgriffe auf Glasfaser oder Satellit unterlaufen, da sie inzwischen alle denkbaren Datenarten umfassen. Die Massenüberwachung entwertet die in nationalen, wie auch in supranationalen Verfassungen und den Menschenrechten niedergelegten[118] Grundwerte und höhlt damit die Basis jeder Demokratie aus. Sie stellt das Verhältnis von Freiheit und Sicherheit, von rechtlichen Befugnissen der Dienste und ihrer parlamentarischen Kontrolle, von notwendigem Geheimschutz und öffentlicher Debatte in Frage. Dieses Verhältnis muss grundlegend und neu hinterfragt werden, insbesondere angesichts der im Untersuchungsausschuss bekanntgewordenen Dimensionen anlassloser, massenhafter Überwachung durch den BND.

6. Massenüberwachung aus US-amerikanischer Sicht

Vor dem Hintergrund der Kooperationen des BND mit der NSA, aber auch der Betroffenheit von Bundesbürger_innen durch Überwachungsmaßnahmen des US-amerikanischen Geheimdienstes, ist ein Blick auf die dortige Debatte um das Thema Massenüberwachung wichtig.

Seit der Aufdeckung der massenhaften Überwachung der NSA 2005 wurde in den Vereinigten Staaten von Amerika ein Prozess der Verrechtlichung begonnen, welcher extra- und illegale Praktiken der NSA gesetzlich absichern sollte.[119] Hierzu wurde der Foreign Intelligence Surveillance Act (FISA) mehrfach geändert[120] und so Ermächtigungsgrundlagen für die NSA geschaffen. Daneben führte die Exekutive mit Billigung

118) U. a. GG, Charta der Grundrechte der EU (Art. 8), EMRK (Art. 8), Zivilrechtspakt des Vertrags über die EU (Art. 16f.), EU-Datenschutzrichtlinie, UN-Menschenrechtscharta (Art. 12); vgl. unten Abschnitt IV.7 Menschenrecht auf Privatheit.

119) Vgl. *Thomas Wischmeyer,* Überwachung ohne Grenzen – Zu den rechtlichen Grundlagen nachrichtendienstlicher Tätigkeiten in den USA, Nomos 2017, S. 21.

120) 2005 durch den USA Patriot Act Improvement and Reauthorization Act, 2007 durch den Protect America Act und 2008 durch den FISA Amendments Act.

des Gesetzgebers aber auch Überwachungsmaßnahmen im Rahmen von sog. Executive Orders fort.[121]

Den rechtlichen Rahmen für eine massenhafte Überwachung im oben erläuterten Sinne setzt dabei in den Vereinigten Staaten der Vierte Zusatzartikel der amerikanischen Verfassung[122], also das berechtigte Vertrauen auf den Schutz der Privatsphäre. Nach der Rechtsprechung des Supreme Courts genießen allerdings lediglich die Inhaltsdaten von US-Personen den Schutz dieses Zusatzartikels. Denn nach der sog. Third-Party-Doctrine können sich Individuen grundsätzlich nicht auf den Vierten Zusatzartikel berufen, soweit sie Dritten freiwillig ihre Daten offenbart haben. Diese Doktrin wird von Behörden und dem United States Foreign Intelligence Surveillance Court (FISC) mit Relevanz für die Programme PRISM und UPSTREAM auch auf E-Mails und Internetkommunikation angewandt.

Die Anfang Juni 2015 beschlossene Reform des Freedom Act enthält lediglich geringfügige Beschränkungen im Hinblick auf die Erfassung insbesondere der Telefonate von US-Bürger_innen. Im Übrigen wurde in den einfachgesetzlichen Regelungen bewusst mit Öffnungsklauseln gearbeitet, um den Diensten die Nutzungsmöglichkeit rechtlicher Grauzonen zu ermöglichen. Die weiteren Änderungen betrafen insbesondere die gerichtliche Kontrolle durch den FISC und die Berichtspflichten der Dienste gegenüber den parlamentarischen Aufsichtsgremien.

In einer sog. Presidential Policy Directive des Weißen Hauses[123] von 2014 wurde zur Bezeichnung einer Massenüberwachung der Begriff der „bulk collection“ verwendet. „Bulk collection“ in diesem Sinne (der Dienste) meint die Sammlung und Speicherung von Daten ohne jegliche Filterung und wird abgegrenzt von „targeted programms“, in welchen Daten von der NSA zwischengespeichert und durchsucht werden oder die mit der Anwendung von Selektoren funktionieren. Diese Auslegung der Begriffe ist freilich

---

121) Vgl. *Thomas Wischmeyer,* Überwachung ohne Grenzen – Zu den rechtlichen Grundlagen nachrichtendienst-licher Tätigkeiten in den USA, Nomos 2017, S. 22.

122) Dieser lautet: „The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.”

123) The White House, Presidential Policy Directive – Signals Intelligence Activities, Policy Directive 28 (Jan. 17, 2014).

wohlfeil, da sie offensichtlich darauf abzielt, die Programme PRISM und UPSTREAM aus der Definition der Massenüberwachung herauszuhalten, obwohl diese doch gerade einer Erfassung von Datenmassen dienen. Dies wird umso deutlicher, als auch die gezielte („targeted“) Überwachung von den Diensten eng ausgelegt wird, um gesetzliche Verbote zu umgehen. Was nach dieser Definition bliebe, sind große Mengen von kollateral abgefangenen Daten, sog. „incidental collection“ welche dann weder ungezielte „bulk collection“ noch gezielte Überwachung sei und damit weder den gesetzlichen Beschränkungen der einen, noch der anderen Sammlung und Speicherung der Daten unterfällt.

PRISM beinhaltet nach dieser Definition keine „unbegrenzte Massenüberwachung“, da die Service Provider zuvor diejenigen Kommunikationsdaten herausfilterten, welche für die Sicherheitsdienste relevant sind und gemäß des Vierten Zusatzartikels rechtmäßig erhoben werden durften. Vor dem Hintergrund der obigen Auslegung des Begriffs der Massenüberwachung würden hier „gezielt“ massenhaft und weltweit Internetnutzer erfasst und kollateral weitere Massen an Kommunikationsdaten von Dritten abgeschöpft.

Die massenhafte Abschöpfung von Kommunikationsdaten im Rahmen des Programs Upstream erfolgt mittels Selektoren, welche den Telekommunikationsunternehmen durch die NSA zugeleitet werden. Hier wird die Problematik, dass eine Zuordnung der Kommunikationsdaten unter den Anwendungsbereich des Vierten Zusatzartikels der Verfassung der Vereinigten Staaten von Amerika kaum erfolgen kann und die massenhafte kollaterale Abschöpfung von Daten Dritter noch deutlicher. Der Abfang sämtlicher Daten ist weder ungezielt, noch handelt es sich bei mittels Selektoren „vorgefilteren“ Abgriffen um eine Art der Überwachung, welche nicht die Charakteristika einer Massenüberwachung hat. Vielmehr kann von Massenüberwachung immer dann gesprochen werden,

> „wenn Daten über eine große Zahl von Personen gleich vollständig ganze Datenstöme „roh“ oder etwa bzw. mit Hilfe weit gefasster Selektoren erhoben werden,

die potentiell auch Personen erfassen können, gegen die keine individualisierten Verdachtsmomente vorliegen." [124]

Der FISC, dem die gerichtliche Kontrolle der Anordnungen zur massenhaften Überwachung oblag, war lange Zeit als „Rubber Stamp Court" verschrien, da er zwischen 1979 und 2012 99,97% der Behördenanträge positiv beschieden hatte.[125] Lediglich 2011 wurde eine Entscheidung veröffentlicht, in welcher Judge *Bates* Teile des UPSTREAM-Programms für verfassungswidrig hielt, da die *NSA* nicht einmal versuchene, die vom Vierten Zusatzartikel geschützte Kommunikation auszusondern.[126]

In einer weiteren Entscheidung des FISC vom 26. April 2017[127] wurde diese Bewertung bestätigt. Das Geheimgericht hatte während des Verfahrens gravierende Bedenken gegenüber der verfassungsmäßigkeit des Programms zum direkten Kabelzugriff der NSA geäußert, welches die sogenannte „about collection" beinhaltet. Bei der „about collection" würden auch die Kommunikationsdaten im Schutzbereich des Vierten Zusatzartikels gesammelt, lediglich weil sie in einer Zielkommunikation erwähnt würden, ohne Sender oder Empfänger zu sein. Die Selektoren und Minimalisierungsregeln der NSA seien zu unspezifisch, als dass sichergestellt werden könnte, dass es sich bei den dabei mitgesammelten Daten Dritter tatsächlich um eine „Incidental Collection" handele.

Diese vom Gericht gerügte massenhafte Sammlung betrifft aber, wie oben dargestellt, lediglich den von dem Vierten Zusatzartikel geschützten Bereich, also die Inhaltskommunikation von US-Personen. Die massenhafte „kollaterale" Abschöpfung der weltweiten Kommunikation Dritter ist nach wie vor ungebremst.

---

124) *Thomas* Wischmeyer, Überwachung ohne Grenzen – Zu den rechtlichen Grundlagen nachrichtendienstlicher Tätigkeiten in den USA, Nomos 2017, S. 16.

125) *Thomas Wischmeyer*, Überwachung ohne Grenzen – Zu den rechtlichen Grundlagen nachrichtendienstlicher Tätigkeiten in den USA, Nomos 2017, S. 29.

126) Foreign Intelligence Surveillance Court, Memorandum Opinion, Docket No. [Redacted] (FISC October 3, 2011) (Bates, J.).

127) Foreign Intelligence Surveillance Court, Memorandum Opinion and Order, Docket No. [Redacted] (FISC April 26, 2017) (Collyer, R. M.).

7. Menschenrecht auf Privatheit

Aufgrund der Art und Weise wie Kommunikation heute funktioniert und organisiert ist, sowie aufgrund global vernetzter Geheimdienste, ist das Recht auf Privatheit besonders auch in seiner menschenrechtlichen Ausprägung bedeutend.

Am 5. Juli 2014 hörte der 1. Untersuchungsausschuss des 18. Deutschen Bundestages auf Grundlage von Beweisbeschluss SV-4 die drei Sachverständigen *Stefan Talmon, Helmut Philipp Aust* und *Douwe Korff* an. Thema der Anhörung war die

> „Regelungslage nach Europarecht und Völkerrecht (einschließlich EMRK und zwischenstaatlicher Abkommen) im Untersuchungszeitraum zur Erhebung, Speicherung auf Vorrat und Weitergabe von Daten aus und über Telekommunikationsvorgänge und Internetnutzung aller Art von Privatpersonen und öffentlichen Stellen durch staatliche Stellen des Bundes oder Stellen der Staaten der sog. Five Eyes bzw. in deren Auftrag handelnde Dritte, einschließlich der Frage, aus welchen Regelungen sich Beschränkungen oder ein Verbot staatlicher Spionagetätigkeit ergeben können oder durch welche Regelungen derartige Tätigkeiten gegebenenfalls legitimiert sind“.[128]

Strittig war während der Anhörung insbesondere der räumliche und persönliche Geltungsbereich des Menschenrechts auf Privatsphäre (Art. 8 der Europäischen Menschenrechtskonvention, EMRK und Art. 17 des Internationalen Paktes über bürgerliche und politische Rechte, IPBPR) und damit die Frage, ob die Überwachung von Ausland-Ausland-Kommunikation sowohl vom Territorium eines Staates aus als auch extraterritorial überhaupt einen Eingriff in das genannte Recht darstellt. Strittig war darüber hinaus die Frage, wann – wenn man einen solchen Eingriff bejahte – eine Menschenrechtsverletzung vorliege, weil die Anforderungen an die Gesetz- und Verhältnismäßigkeit von Überwachungsmaßnahmen verfehlt würden. Für die Internet- und Telekommunikationsüberwachung durch Geheimdienste fehle es, so der Sachverstän-

---

128) Beweisbeschluss SV-4.

dige *Talmon*, an „aussagekräftigen Entscheidungen“ des zur Überwachung der Einhaltung des IPBPR berufenen Menschenrechtsausschusses der Vereinten Nationen.[129]

Drei Monate zuvor hatte der UN-Menschenrechtsausschuss in seinen abschließenden Bemerkungen zum Staatenbericht der USA die bekannt gewordenen Überwachungsprogramme der NSA und das mangelhafte Aufsichtsregime deutlich kritisiert. Gerügt wurde, dass auch mit der sog. Presidential Policy Directive 28 die Diskriminierung von Nicht-US-Bürger_innen fortbestehe, die Gerichtsbarkeit des Foreign Intelligence Surveillance Court im Geheimen stattfinde und das Kontrollregime einen effektiven Rechtsschutz für betroffene Personen verfehle. Die USA wurden aufgefordert ihre menschenrechtlichen Verpflichtungen einzuhalten:

> „[M]easures should be taken to ensure that any interference with the right to privacy complies with the principles of legality, proportionality and necessity, regardless of the nationality or location of the individuals whose communications are under direct surveillance, regardless of the nationality or location of the individuals whose communications are under direct surveillance“.[130]

Das klare Bekenntnis des Ausschusses zur staatlichen Pflicht, das Menschenrecht auf Privatheit auch extraterritorial zu achten, erläuterte ein nur wenige Tage vor der Sachverständigenanhörung veröffentlichter Bericht der damaligen UN-Menschenrechtskommissarin *Navi Pillay* wie folgt:

> „Der Menschenrechtsausschuss hat sich von dem schon in seinen frühesten Entscheidungen geäußerten Grundsatz leiten lassen, dass ein Staat sich seinen Verpflichtungen auf dem Gebiet der internationalen Menschenrechte nicht entziehen kann, indem er außerhalb seines Hoheitsgebiets Maßnahmen vornimmt, die ihm „im eigenen Land“ untersagt wären. […] Die Begriffe ‚Gewalt‘ und ‚tatsächliche Kontrolle‘ [in

129) Talmon 2014, S. 50.

130) Human Rights Committee 2014, Rn. 22a.

> Art. 2 IPBPR zum Anwendungsbereich des Paktes] sind Indikatoren dafür, ob ein Staat ‚Herrschaftsgewalt' oder hoheitliche Befugnisse ausübt, deren Missbrauch durch Vorschriften zum Schutz der Menschenrechte eingeschränkt werden soll. Ein Staat kann sich seinen menschenrechtlichen Verantwortlichkeiten nicht einfach dadurch entziehen, dass er es unterlässt, Befugnisse dieser Art rechtlich einzugrenzen. Ein anderer Schluss würde nicht nur die Universalität und den Wesensgehalt der durch die internationalen Menschenrechtsnormen geschützten Rechte untergraben, sondern möglicherweise auch strukturelle Anreize für Staaten schaffen, Überwachungsaktivitäten wechselseitig auszulagern. Daraus folgt, dass digitale Überwachungsmaßnahmen die Menschenrechtsverpflichtungen eines Staates berühren können, wenn die Überwachung mit der Ausübung staatlicher Gewalt oder tatsächlicher Kontrolle in Bezug auf digitale Kommunikationsinfrastruktur, gleich wo sich diese befindet, durch den Staat verbunden ist, beispielsweise durch direktes Abhören oder durch Eindringen in diese Infrastruktur."[131]

Entsprechend mahnte der Menschenrechtsausschuss gegenüber den USA an, dass Eingriffe in das Recht auf Privatsphäre nur spezifischen legitimen Zwecken dienen dürfen. Die Eingriffsnormen müssen öffentlich zugänglich und hinreichend bestimmt sein, d. h. sie sollen

> „specify in detail the precise circumstances in which any such interference may be permitted, the procedures for authorization, the categories of persons who may be placed under surveillance, the limit and duration of surveillance; procedures for the use and storage of data collected".[132]

131) Human Rights Council 2014, Rn. 32 f.

132) Human Rights Committee 2014, Rn. 22 b.

Diese Position zu Programmen (extraterritorialer) Massenüberwachung hat der UN-Menschenrechtsausschuss seitdem wiederholt in Staatenberichtsverfahren bekräftigt, u. a. auch gegenüber den drei *Five Eyes-Staaten* Kanada, Neuseeland und dem Vereinigten Königreich.[133] In diesem Zusammenhang forderte der UN-Menschenrechtsausschuss zudem die wirksame Kontrolle des Austauschs von personenbezogenen Informationen („Rohdaten") zwischen Geheimdiensten, um sicherzustellen, dass daraus keine Menschenrechtsverletzungen resultieren.

Daneben haben in den drei Jahren seit der Sachverständigenanhörung auch verschiedene vom UN-Menschenrechtsrat eingesetzte Sonderberichterstatter_innen das Thema Massenüberwachung aufgegriffen. So beklagte etwa *Ben Emmerson*, Berichterstatter für den Schutz der Menschenrechte in der Terrorismusbekämpfung, im Februar 2017, dass auch die jüngsten Entscheidungen von EuGH (Urteil in den Fällen Tele2 Sverige AB v. Post-och telestyrelsen und Secretary of State for the Home Department v. Tom Watson and Others vom 21. Dezember 2016) und EGMR (Urteile im Fall Zakharov v. Russia vom 4.12.2015 und im Fall Szabo and Vissy v. Hungary vom 12.1.2016) zur gebotenen Verhältnismäßigkeit von Kommunikationsüberwachung nicht wirklich zu einer Begrenzung von Programmen extraterritorialer Überwachung geführt haben. Mit ausdrücklichem Verweis auch auf das deutsche Gesetz zur Ausland-Ausland-Fernmeldeaufklärung des BND erinnert er daran, dass die rechtliche Ungleichbehandlung von Ausländer_innen unvereinbar mit dem Nichtdiskriminierungsprinzip ist. Auch wenn er die rechtliche Normierung von bis dato unregulierten Überwachungspraktiken als Fortschritt sieht, sei diese allein nicht hinreichend, um die Vereinbarkeit mit völkerrechtlichen Verpflichtungen zu gewährleisten:

> „Necessity, proportionality and non-discrimination must also be taken into account, along with the establishment of safeguards against arbitrariness, independent oversight and routes for redress."[134]

---

133) Human Rights Committee 2015a, Rn. 10; Human Rights Committee 2015b, Rn. 24; Human Rights Committee 2016 b, Rn. 15-16; vgl. auch Human Rights Committee 2016a, Rn. 36-37.

134) Human Rights Council 2017a, Rn. 36.

Ähnlich bewertete auch *Joseph Cannataci*, der erste Sonderberichterstatter für das Recht auf Privatsphäre, die gesetzgeberischen Aktivitäten in verschiedenen Ländern. Bezugnehmend auf die mittlerweile drei Resolutionen der UN-Generalversammlung zum „Recht auf Privatsphäre", in denen diese die Staaten zur Revision von Recht und Praktiken der Kommunikationsüberwachung auffordert, konstatiert er:

> „The states that reacted, started to work on and pass new laws on the subject that only, if at all, contain minor improvements in limited areas. In general, these laws have been drafted and rushed through the legislative process with political majorities to legitimize practices that should never have been implemented." [135]

Seine Kritik gilt dabei nicht nur dem fehlenden Nachweis der Wirksamkeit und der Unverhältnismäßigkeit der Maßnahmen, sondern auch einem Ansatz, der – anstatt auf internationale Instrumente der Kriminalitäts- und Terrorismusbekämpfung zu setzen – dem Konzept nationalstaatlicher Souveränität verpflichtet sei.

Wenngleich die diversen Stellungnahmen kein völkerrechtliches „hard law" darstellen, so zeigt sich doch, dass das Recht auf digitale Privatsphäre seit den *Snowden*-Enthüllungen zu einer Priorität für die Einrichtungen des UN-Menschenrechtssystems geworden ist. Sowohl die autoritative Interpretation von Art. 17 IPBR durch den UN-Menschenrechtsausschuss als auch andere Expert_innen machen seither regelmäßig deutlich, dass das Menschenrecht auf Privatsphäre durch die Staaten sowohl gegenüber Ausländer_innen als auch extraterritorial zu achten ist. Jeder Eingriff – durch die Datenerhebung selbst und auch die Weitergabe von Informationen – muss dabei rechtmäßig, hinreichend bestimmt geregelt und verhältnismäßig sein sowie wirksam kontrolliert werden.

135) Human Rights Council 2017b, Rn. 13.

V. Kooperation des BND mit der NSA: EIKONAL und Bad Aibling

1. Memorandum of Agreement (MoA) vom April 2002

Das Memorandum of Agreement (MoA) vom 28. April 2002 zwischen BND und NSA ist die vertragliche Grundlage für deren problematische Zusammenarbeit in Deutschland seither bei der Überwachung von Satelliten- und Kabel-gestützter Telekommunikation. Strukturen, Umfang und Exzesse dieser Kooperation haben *Edwards Snowdens* Veröffentlichungen sowie vertiefend auch dieser 1. Untersuchungsausschuss des Bundestags beleuchtet.

Zu diesem Zweck versuchte der UA zunächst, sich bezüglich des MoA zutreffende Kenntnis zu verschaffen über Motive und Interessen für dessen Abschluss sowie über dessen Inhalte.[136]

a) Inhalt des MoA

Diese Erkenntnisse können hier leider nicht detailliert wiedergegeben werden, weil das MoA selbst VS-GEHEIM ist und dessen fünf Annexe VS-STRENG GEHEIM.[137]

Doch Medien gaben einzelne Inhalte dieser MoA-Anhänge wieder. Demnach

> „verständigen sich beide Seiten auf gemeinsame Spionagethemen und -ziele, wie die Bekämpfung von Terrorismus, organisierter Kriminalität und der Verbreitung von Massenvernichtungswaffen. (…) Grundrechte wie das Brief-, Post- und Fernmeldegeheimnis [seien] zu achten, mithin keine Deutschen und keine Amerikaner auszuforschen. Das gelte für ‚reale' und ‚juristische Personen', also Firmen oder Verbände. [Doch es gäbe] Ausnahmen (…) im Falle ‚terroristischer Aktivitäten' ist das Tabu kein Tabu mehr. Wenn sich bei abgefangenen Signalen brisanten Inhalts im Nachhinein herausstellt, dass sie von

---

136) Vgl. die Darstellung im Feststellungsteil F.III.5.

137) MAT A BK-4/1 (Tgb.-Nr. 1/14 – STRENG GEHEIM), Bl. 45 ff. (GEHEIM und STRENG GEHEIM); laut *Spiegel Online* vom 15. Juni 2014 umfasst das MoA nur 6 und die Anhänge 74 Seiten, http://www.spiegel.de/politik/deutschland/mehr-als-200-us-geheimdienstler-spionieren-offiziell-in-deutschland-a-975285.html [letzter Abruf: 16. Juni 2017].

> einem Deutschen stammen, können sie trotzdem verwendet werden – wenn der Partner informiert wird und seine Zustimmung erteilt. Das Gleiche gilt, wenn sich die ‚Endpunkte' der belauschten Kommunikation im jeweils anderen Land befänden."[138]

Den BND-Zeugen *R. U.* verstanden wir dahingegehend, dass er die Existenz solcher Ausnahmen im MoA bei seiner öffentlichen Zeugenbefragung inzident einräumte:

Auf Frage des Abgeordneten *Roderich Kiesewetter*: „Sieht das Abkommen nach Ihrer Kenntnis – das eben diese Zusammenarbeit regelt – Ausnahmen für den Informationsaustausch vor, mit dem die gesetzlichen Vorgaben, G 10, umgangen werden können?"

> *R. U.*: „Solche Details kann ich in einer öffentlichen Sitzung nicht beantworten." [139]

Auf Frage des Abgeordneten *Burkhard Lischka*: „Einmal zur G-10-Filterung (…) Werden denn die Daten irgendwie darüber hinaus noch gefiltert, also beispielsweise um Daten von US-Bürgern bereinigt und (…) möglicherweise (…) hinsichtlich aller EU-Bürger oder nicht?"

> *R. U.*: „Da würde ich auch bitte wieder auf die nichtöffentliche Sitzung verweisen."[140]

Auch der ehemalige BND-Präsident *Schindler* bezeugte, dass Annex I des MoA – das „Betriebskonzept" – unter Nummer 1.3.2 die Aufklärung europäischer Ziele zulässt (ohne dass der Datenfilter DAFIS dies prüfen konnte):

> „Was DAFIS eben nicht kann, ist die Prüfung von europäischen Kriterien, und zwar die Prüfung der Übereinstimmung mit dem Betriebskonzept, dem Annex 1 zum MoA von 2002 und dort die Nummer 1.3.2,

138) *Der Spiegel* vom 16. Juni 2014, „Eifer und Gier".

139) *R. U.*, Protokoll-Nr. 14 I, S. 26.

140) *R. U.*, Protokoll-Nr. 14 I, S. 18 f.

> nämlich dass europäische Ziele nur unter bestimmten Voraussetzungen aufgeklärt werden dürfen. Und das konnte und kann DAFIS überhaupt nicht prüfen.“[141]

Ferner erklärte der Zeuge *Schindler* über den Inhalt des Annex II des MoA,

> „wo im MoA ja die Rechtstaatlichkeit in Annex 2 festgeschrieben ist (...) lang und breit im Annex 2 des MoA geregelt (…) Deutsche sind ja per se erst mal geschützt im Annex 2, genauso wie US-Bürger, wenn eine solche zufällige Erfassung stattfindet –, sie nach G 10 behandelt werden muss.“[142]

Der BND-Zeuge *R. U.* berichtete über Inhalte des MoA (das er ‚MoU‘ nannte):

> „Da werden ja (…) geregelt unter anderem die ganzen Filtermechanismen, dass es eben G-10-Filterung gibt, dass es auch im Gegenzug – damals mit der gemeinsamen Zusammenarbeit – eine amerikanische Filterung gab, eine USSID 18 nannte sich das. (…) wer welche Infrastrukturkosten bezahlt, wer für Technik zuständig ist, wer zum Beispiel mit der Leitung dieses gemeinsamen Sachgebietes betraut ist; das war immer ein Deutscher, und der Vertreter war immer ein Amerikaner. Solche Grundzüge waren in dem MoU enthalten.“ [143]

Die „Vertrauensperson“ der Bundesregierung, *Graulich*, gab in ihrer Stellungnahme einen kursorischen Überblick über Inhalt des MoA nebst Anhängen.[144]

---

141) *Schindler,* Protokoll-Nr. 54 I, S. 30.

142) *Schindler,* Protokoll-Nr. 54 I, S. 11, 44.

143) *R. U.*, Protokoll-Nr. 14 I, S. 26.

144) *Graulich*, Bericht vom 23. Oktober 2015, MAT A SV-11/2, S. 81-97.

2013 zitierte der Kanzleramtsminister *Pofalla* angeblich wörtlich aus der Einleitung des MoA – wiewohl streng geheim – die dortigen Wohlverhaltens-Abreden, etwa zur Einhaltung deutscher Gesetze.[145]

Die BfDI hat sich in ihrem Sachstandsbericht vom 30. Juli 2015 zur BND-/NSA-Kooperation in Bad Aibling nebst zugehöriger rechtlicher Bewertung vom 15. März 2016 ebenfalls kritisch mit dem MoA als deren Grundlage befasst.[146] So kritisierte sie, dass offenbar der Annex III (Punkt 5.3.2) die Geltung des Bundesdatenschutzgesetzes bzw. dessen Datenübermittlungs-Vorschriften abbedingen und ersetzen wolle. Ferner kritisierte die BfDI, dass weder im MoA noch anderswo der BND der NSA vor Aufnahme der Überwachungs-Zusammenarbeit in Bad Aibling auferlegt habe, Zugangsrecht und Kontroll-Kompentenz der BfDI anzuerkennen und zu unterstützen.[147] Außerdem kritisierte die BfDI die vom BND in Bad Aibling praktizierte „Prüfung und Genehmigung von Zutrittsberechtigungen für das NSA-Personal entsprechend des im MoA festgelegten Verfahrens (MOA, Annex V, 4.1)“.[148]

b) Ziel der NSA bei Abschluss und Durchführung des MoA

Wir haben aufgrund unserer Sichtung der Akten, ohne deren Details hier wiedergeben zu dürfen, Anlass zu der Annahme, dass die NSA mit ihrem – Mitte 2001 überraschenden[149] – Angebot eines MoA vor allem darauf zielte, Zugang zur Erfassung von kabelgestützter Telekommunikation am Frankfurter Kabelknoten zu bekommen und damit

145) Pressestatement von Kanzleramtsminister *Pofalla* nach der Sitzung des Parlamentarischen Kontrollgremiums am 12. August 2013, darin Ziffer 1, https://www.bundesregierung.de/ContentArchiv/DE/Archiv17/Mitschrift/Pressekonferenzen/2013/08/2013-08-12-pofalla.html [letzter Abruf: 16. Juni 2017], („Bereits in einem MoA (...) vom 28. April 2002 hat die NSA versichert, und ich muss wieder zitieren: „Die NSA erklärt ihr Einverständnis, sich an die deutschen Gesetze und Bestimmungen zu halten.“)

146) Vgl. die Erwähnung dieses Sachstandsberichts in der Rechtlichen Bewertung der BfDI vom 15. März 2016, https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/#Teil-1-A-VI-1-a [letzter Abruf: 16. Juni 2017].

147) BfDI, Rechtliche Bewertung vom 15. März 2016, https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling, dort unter Suchwort „MoA“ [letzter Abruf: 16. Juni 2017].

148) BfDI, Rechtliche Bewertung vom 15. März 2016, https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling, dort unter Suchwort „MoA“ [letzter Abruf: 16. Juni 2017].

149) Vgl. die im Feststellungsteil F.III.5 unter a) zitierten Zeugenaussagen damals Beteiligter.

Zugang zu europäischen Glasfaserkabeln zu erhalten: so wie dies später real mit der Operation EIKONAL dort praktiziert wurde. Diese Motivation hielten auch die ab Sommer 2001 mit den Verhandlungen befassten Zeugen aus BND und Bundeskanzleramt für möglich bis naheliegend. Ab wann der BND und auch das Bundeskanzleramt diese Motivation als sicher erkannten und billigten, können wir nicht exakt terminieren; sie war aber ausweislich der Akten dem BND-Präsidenten vor Unterzeichnung des MoA am 28. April 2002 bekannt.[150]

Dieses Bestreben hat der ehemalige Präsident des österreichischen Verfassungsschutzes, *Gert Polli*, dahin bewertet, die NSA habe „Deutschland über den Tisch gezogen“:[151]

> „In der NSA-Affäre hat man dem BND vorgeworfen, die Politik nur unzureichend über die Kooperation mit der NSA informiert zu haben. Aus meiner Sicht hat die NSA die Kooperation mit dem BND bewusst überspannt und damit auch Deutschland über den Tisch gezogen. Es ist richtig, dass der BND sich nach 09/11 zu stark auf die NSA, aber auch auf die Zusammenarbeit mit der CIA abgestützt hat. Die Leiter dieser Behörde konnten jedoch davon ausgehen, dass die enge Kooperation mit der NSA politisch gewollt und damit abgesegnet war. Dass das Kanzleramt im Nachhinein davon spricht, nicht ausreichend informiert worden zu sein, ist nur die halbe Wahrheit.“

Die „Vertrauensperson“ der Bundesregierung, *Graulich*, stellte in ihrem Schlussbericht ähnlich fest, die NSA habe „qualitativ gravierende Verstöße“ gegen das MoA begangen, sich damit „nicht nur vertragswidrig verhalten“, sondern „bündnispolitisch prekär“

150) *Fechner*, Protokoll-Nr. 41 I, S. 20 f.; *Breitfelder*, Protokoll 30 II – Auszug offen, S. 73 f., 94.

151) *Gert R. Polli*, „Die NSA hat Deutschland über den Tisch gezogen“, http://www.gertpolli.com/en/gert-polli/articles-en/55-“die-nsa-hat-deutschland-über-den-tisch-gezogen“.html [letzter Abruf: 16. Juni 2017].

auch „die deutsche Position gegenüber ihren europäischen Partnern potentiell gefährdet“.[152]

c) MoA als Rechts-/Arbeitsgrundlage bei Umsetzung im BND ignoriert

Wir haben den Eindruck gewonnen, dass die Sachbearbeiter des BND bis in Leitungsebenen hin Inhalte, Vorgaben und Begrenzungen des MoA bei dessen praktischer Umsetzung mit der NSA entweder nicht kannten oder aber jedenfalls ignorierten, erst recht nicht im Detail die für Datenerfassung und -Übermittlung eigentlich maßgeblichen Gesetzesgrundlagen (v. a. Artikel 10-Gesetz, BDSG, BNDG mit Verweis auf BVerfSchG). Dieser Befund entspricht nach der Vernehmung zahlreicher BND-Zeugen demjenigen zum Auftragsprofil der Bundesregierung (APB), welches als entscheidende Arbeitsgrundlage des BND dort ebenso unbekannt war bzw. praktisch ignoriert wurde.

Dieser erschreckende Zustand wurde mitverursacht dadurch, dass weder die Fachaufsicht des Bundeskanzleramts noch die BND-Spitze spezifische Weisungen erließ für die praktische Umsetzung des MoA. Folglich blieb dies den Sachbearbeitern und Anwendern im BND unklar, so dass diese weitgehend nach Gutdünken verfahren mussten bzw. konnten.

d) Parlamentarisches Kontrollgremium über MoA nicht, zu spät und zu wenig informiert

Die Bundesregierung war seit jeher verpflichtet, das Parlamentarische Kontrollgremium des Bundestages für die Kontrolle der Nachrichtendienste (PKGr) „umfassend über die allgemeine Tätigkeit“ der Nachrichtendienste „und über Vorgänge von besonderer Bedeutung“ zu unterrichten.[153]

Wir haben Anlass zu der Annahme, dass die Bundesregierung diese Unterrichtungspflicht verletzt hat bzgl. Abschluss des MoA durch den BND sowie der sukzessiven

---

152) Zitiert nach *Süddeutsche.de* vom 30. Oktober 2015, „NSA jubelte BND deutsche Spähziele unter“, http://www.sueddeutsche.de/politik/geheimdienst-affaere-nsa-jubelte-bnd-deutsche-spaehziele-unter-1.2715253 [letzter Abruf: 16. Juni 2017]; Zur NSA-Selektorenproblematik siehe Abschnitt V.8. Verstöße bei Verwendung von NSA-Selektoren.

153) So § 4 PKGrG seit 1999; früher entsprechend gemäß § 2 PKK-G.

Umsetzung des MoA. Dies waren zweifellos „Vorgänge von besonderer Bedeutung“, welche die Unterrichtungspflicht auslösten.

Ob solche Unterrichtungen des PKGr überhaupt erfolgten, wie Regierungsvertreter gern behaupten, ob dies real unterblieb oder ggf. wann und wie sie erfolgten: All das darf hier nicht dargestellt werden, weil es der Geheimhaltungspflicht des PKGr über derlei unterliegt.[154]

Dass solche Unterrichtungen des PKGr erfolgt seien, ergibt sich jedenfalls weder aus dessen regelmäßig veröffentlichten Tätigkeitsberichten[155] noch aus denjenigen über die Durchführung des G10[156] im vor allem relevanten Zeitraum 2001 – 2009.

Gleiches gilt für die öffentliche Behauptung des ex-Kanzleramts *Pofalla* (ungeachtet der auch für ihn geltenden Geheimhaltungspflicht gemäß § 10 PKGrG), das PKGr sei „seit 1998“ bis Juni 2013 „bereits siebenundzwanzig Mal über Fragen der Zusammenarbeit mit den USA, Datentransfer oder Bad Aibling informiert worden“.[157]

---

154) § 10 PKGrG.

155) Bericht über die Kontrolltätigkeit gemäß § 6 des Gesetzes über die parlamentarische Kontrolle nachrichtendienstlicher Tätigkeit des Bundes: Bericht vom 2. Dezember 2004 (Berichtszeitraum: August 2002 bis Oktober 2004), http://dipbt.bundestag.de/doc/btd/15/044/1504437.pdf; Bericht vom 8. Mai 2005 (November 2004 bis September 2005), http://dip21.bundestag.de/dip21/btd/15/059/1505989.pdf; Bericht vom 12. Dezember 2007 (Berichtszeitraum: Oktober 2005 bis Dezember 2007), http://dip21.bundestag.btg/dip21/btd/16/075/1607540.pdf; Bericht vom 31. August 2009 (Berichtszeitraum Januar 2008 bis August 2009), http://dip21.bundestag.btg/dip21/btd/16/139/1613968.pdf.

156) Bericht gemäß § 14 Abs. 1 Satz 2 des Gesetzes zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10-Gesetz – G10) über die Durchführung sowie Art und Umfang der Maßnahmen nach den §§ 3, 5 und 8 dieses Gesetzes: 1) Bericht vom 24. März 2003 (Berichtszeitraum 1. Juli 2001 – 30. Juni 2002), Bundestagsdrucksache 15/718, http://dipbt.bundestag.de/doc/btd/15/007/1500718.pdf; 2) Bericht vom 4. März 2004 (Berichtszeitraum 1. Juli 2002 bis 30. Juni 2003), Bundestagsdrucksache 15/2616, http://dipbt.bundestag.de/doc/btd/15/026/1502616.pdf; 3) Bericht vom 2. Mai 2005 (Berichtszeitraum 1. Juli 2003 bis 30. Juni 2004), Bundestagsdrucksache 15/4897, http://dipbt.bundestag.de/doc/btd/15/048/1504897.pdf; 4) Bericht vom 7. September 2006 (Berichtszeitraum 1. Juli 2004 bis 31. Dezember 2005), http://dip21.bundestag.btg/dip21/btd/16/025/1602551.pdf; 5) Bericht vom 25. Juni 2007 (Berichtszeitraum 1. Januar 2006 bis 31. Dezember 2006), http://dip21.bundestag.btg/dip21/btd/16/068/1606880.pdf; 6) Bericht vom 5. Januar 2009 (Berichtszeitraum 1. Januar 2007 bis 31. Dezember 2007), http://dip21.bundestag.btg/dip21/btd/16/115/1611559.pdf.

157) So in Pressestatement von Kanzleramtsminister *Pofalla* nach der Sitzung des Parlamentarischen Kontrollgremiums am 12. August 2013, darin Ziffer 10, https://www.bundesregierung.de/ContentArchiv/DE/Archiv17/Mitschrift/Pressekonferenzen/2013/08/2013-08-12-pofalla.html [letzter Abruf: 16. Juni 2017].

Tatsächlich liegt nahe, dass in diesen 15 Jahren die Bundesregierung mal irgendwelche Aspekte der „Zusammenarbeit mit den USA, Datentransfer oder Bad Aibling“ berichtet haben wird, doch mutmaßlich nicht genauer über das MoA, geschweige über den Kabelzugriff zugunsten des NSA. Es erscheint zwar nicht ausgeschlossen, dass den Regierungsvertretern Informationen auch dazu bisweilen auf ihre sogenannten Sprechzettel für Regierungsvertreter für PKGr-Sitzungen geschrieben worden sind (womöglich mit dem Zusatz „nur reaktiv“). Doch dies garantiert keineswegs, dass die Sitzungsvertreter der Bundesregierung dies dann in den Sitzungen tatsächlich initiativ vorgetragen haben.

Seit einigen Jahren ist in der Geschäftsordnung des Parlamentarischen Kontrollgremiums konkretisiert, dass die Bundesregierung das PKGr zu unterrichten hat über „Vereinbarungen über neue Kooperationen von grundlegender Bedeutung“ wie das MoA.[158]

aa) Bundesregierung verschwieg Umfang der Kooperation bei Satelliten-Überwachung v. a. bezüglich Afghanistan

Wir stellen nach der Beweisaufnahme fest – ohne dies aus geheimen Akten spezifizieren zu dürfen –, dass NSA und BND sehr intensiv kooperierten u. a. bei der Überwachung Satelliten-gestützter Telekommunikation in/aus Afghanistan, auch wegen des Interesses dortiger US-Militärs hieran, und dabei regelmäßig Hunderte Millionen personenbezogener Datensätze erfassten. Mutmaßlich erfuhren die Betroffenen (in Afghanistan und deren Kommunikationspartner außerhalb Afghanistan) hiervon wie so oft nichts.

Die Bundesregierung unterrichtete den Bundestag von den Ausmaßen dieser Überwachung pflichtwidrig nicht.

---

158) Anlage zu § 4 GO PKGrG, Ziffer 2, Anstrich 2, http://www.bundestag.de/blob/366638/a85399f8781425f72cb0158d59ba56bf/go_pkgr-data.pdf, [letzter Abruf: 16. Juni 2017].

bb) Bundesregierung täuschte Bundestag über Erfassungen am Frankfurter Kabelknoten der *Deutschen Telekom* sowie über Weitergabe dort gewonnener Daten an die NSA

Wir haben – ohne dies aus geheimen Akten spezifizieren zu dürfen – Anlass zu der Annahme, dass die Bundesregierung dem Bundestag die Kommunikations-Erfassungen am Frankfurter Kabelknoten der *Deutschen Telekom* sowie die Weitergabe dort gewonnener Daten an die NSA nicht nur verschwieg, sondern den Bundestag darüber richtiggehend täuschte, z. B. dessen G 10-Kommission.[159] So konnte der Bundestag nicht die Dimension dieser u. E. rechtswidrigen Praxis erkennen.

Selbst wenn es z. B. an diesem Kabelknoten zu einem brisanten Vollzugriff des BND auf sämtliche dort durchfließenden Telekommunikationsverkehre gekommen *wäre* (sogen. „Full Take“), etwa um die Werthaltigkeit und Zusammensetzung dieser Verkehre in der Frühphase vor Beginn dieses Überwachungsvorhaben zu analysieren, dann hätte die Bundesregierung gewiss immer noch keinen Anlass gesehen, den Bundestag und die BfDI hiervon zu unterrichten, also in welche Richtung diese Praxis sich entwickeln kann.

e) Rechtliche und politische Bewertung des MoA

Für die stattgefundene Datenerfassung von BND und NSA sowie deren Übermittlung untereinander konnte nur deutsches Recht der Maßstab und Grundlage sein, also nicht etwa verdrängend das MoA.

Dieses verkannte u. a. der BND-Zeuge *R. U.*, ehemaliger Dienststellenleiter von Bad Aibling, der das MoA als eigentliche Rechtsgrundlage für Datenübermittlungen des BND an die NSA erachtete:

> auf Frage des Abgeordneten *Burkhard Lischka*: „Auf welcher Rechtsgrundlage werden eigentlich die Daten weitergeleitet an die USA?“
>
> *R. U.*: „Basierend auf dem MoU, das 2002 geschlossen wurde.“[160]

---

159) Vgl. gesonderte Darstellung dazu in Abschnitt V.4 – G10-AO als Türöffner.

160) *R. U.*, Protokoll-Nr. 14 I, S. 19.

Dies verkannte ebenso die Vertrauensperson der Bundesregierung, *Graulich*, die in ihrer Stellungnahme das MoA einordnete als einen „Durchleitungsvertrag“ mit einer „abdrängenden Verantwortlichkeit“, nämlich dass die datenschutzrechtliche Verantwortung für (…) die Rechtmäßigkeit der Erhebung, die Zulässigkeit der Eingabe sowie die Richtigkeit oder Aktualität der Daten, (…) für den Betrieb der Anlage und den gesteuerten Inhalt, nämlich die Selektoren (…) deren jeweiligen Urhebern“ allein obliege: also insoweit allein der NSA.[161]

Zum Rechtscharakter des MoA im Übrigen urteilte der ehemalige BND-Präsident *Schindler*, dass

> „ein MoA oder MoU (…) ja einen deutlich niederen Rechtscharakter hat [als ein] völkerrechtlichen Vertrag“.[162]

Auch das Bundeskanzleramt meinte,[163] es handele sich weder um eine völkerrechtliche Vereinbarung, die der Aufbewahrung im politischen Archiv des Auswärtigen Amts würdig sei,[164] noch um einen der Zustimmung des Bundestages bedürftigen Vertrag zur Regelung politischer Beziehungen des Bundes.[165]

Das beurteilen wir anders.

aa) MoA ist kein bloßes Verwaltungsabkommen und wäre als solches auch unwirksam

Das MoA ist unbestritten auch nach Auffassung der Bundesregierung ein zwischenstaatlicher völkerrechtlicher Vertrag im Sinne des Art. 59 Abs. 2 Grundgesetz. Rechtswirkung maß die Bundesregierung dem MoA u.a. schon deshalb bei, weil darin die US-Seite ihre Bindung an deutsches Recht und Gesetz wie verlangt anerkannte.

161) *Graulich*, Bericht vom 23. Oktober 2015, MAT A SV-11/2, S. 80.

162) *Schindler*, Protokoll-Nr. 54 I, S. 24.

163) Vermerk des Bundeskanzleramtes, Referat 601 vom 10. September 2013, MAT A BK-1/1a_7, Bl. 273 (VS-NfD).

164) Gemäß § 10 GAD, http://www.gesetze-im-internet.de/gad/__10.html.

165) Gemäß Art. 59 Abs. 2 GG, http://www.gesetze-im-internet.de/gg/art_59.html.

Das MoA ist real kein bloßes Verwaltungsabkommen gemäß Satz 2 jener Norm, dessen Abschluss keiner parlamentarischen Beteiligung bedurft hätte. So allerdings handhabte es 2002 die Bundesregierung, um die Mitwirkung des Bundestages fernzuhalten.[166] Das war u. E. schon formell unzulässig. Denn der Abschluss eines solchen Verwaltungsabkommens hätte einer Ermächtigung des Bundespräsidenten bedurft; dies ergibt sich schon klar aus dem Wortlaut des Art. 59 Abs. 1 S. 2 GG. Argumentative Versuche, die entgegengesetzte Regierungspraxis zu rechtfertigen durch eine unterstellte „stillschweigende Ermächtigung" des Bundespräsidenten,[167] vermögen nicht zu überzeugen. Eine solche Ermächtigung hat der Bundespräsident in allgemeiner Form erst mit Schreiben vom 11. August 2004 erteilt,[168] also erst nach Abschluss des MoA.

Abgesehen davon hätte das MoA als ein angenommenes Verwaltungsabkommen aber zumindest einer Zustimmung des Bundesministers des Auswärtigen bedurft.[169] Solche förmliche Zustimmung des AA indes unterblieb unseres Wissens damals aber. Folglich war bzw. wäre das MoA als Verwaltungsabkommen schon formell unwirksam.

aaa) Das MoA als politischer Regelungs-Vertrag

Wir hingegen beurteilen das MoA als Vertrag zur Regelung politischer Beziehungen des Bundes sowie zugleich mit innerstaatlichen Rechtswirkungen: also gemäß beiden Alternativen des Art. 59 Abs. 2 S. 1 GG. Diese beiden, je Parlamentsbeteiligung auslösenden Voraussetzungen können nebeneinander zugleich erfüllt sein.[170]

---

166) Sehr kritisch zu solcher Neigung der Regierungspraxis: *Maunz/Dürig/Nettesheim*, 78. Ergänzungslieferung September 2016, GG Art. 59, Rn. 101, FN 3 m. w. N: am Beispiel von militärischen Ausrüstungshilfeabkommen.

167) So allerdings – jedenfalls noch 1984 – auch BVerfGE 68, 1 (82 f. = Rn. 136); dagegen äußert etwa *Michael Schweitzer* (Staatsrecht, Völkerrecht, Europarecht, 2010, S. 55 f, Rn. 135 ff. „erhebliche verfassungsrechtliche Bedenken", „Verschiebung des Kompetenzgefüges ist mit Art. 79 Abs. 1 GG nicht vereinbar"; „nicht überzeugt" auch *Pieper,* in: Beck'scher Online-Kommentar (BeckOK) GG/*Pieper*, [32. Ed. 1. März 2015], GG Art. 59 Rn. 45.1 mit Verweis auf die ja bestehende explizite Delegationsmöglichkeit in Art. 60 Abs. 3 GG; generell ablehnend auch Calliess in: Isensee, Kirchhoff (Hrsg.), Handbuch des Staatsrechts der BRD, Band IV, 2006 § 83 Rn. 19.

168) Zitiert nach *Pieper* in BeckOK GG/*Pieper*, [32. Ed. 1. März 2015], GG Art. 59, Rn. 46.

169) Gemäß § 72 Abs. 2 GGO iVm § 11 Abs. 2 GOBReg; ebenso *Pieper* in BeckOK GG/*Pieper*, [32. Ed. 1. März 2015], GG Art. 59, Rn. 46; vgl. BVerfG, LKV 2007, 509 (510 aE) [„...formal wirksam in die deutsche Rechtsordnung transformieren"]; weitere Nachweise bei *Fastenrath*, DÖV 2008, S. 697 (700, Rn. 38 f.)

170) Vgl. nur *Maunz/Dürig/Nettesheim*, 78. Ergänzungslieferung September 2016, GG Art. 59, Rn. 103 mwN.

Das MoA regelt machtpolitische Beziehungen des Bundes im Sinne der Alternative 1 dieser Norm: nämlich ein sicherheitspolitisches Bündnis mit den USA zur gemeinsamen Telekommunikationsüberwachung in Deutschland (Bad Aibling, Frankfurt u. a.) sowie von dort mit Wirkung im Ausland, etwa erklärtermaßen in Afghanistan zum Schutz deutscher und US-amerikanischer Truppen dort. Damit bereits erfüllt das MoA selbst die enge – oft als zu eng und überholt kritisierte[171] – historische Interpretation dieser Voraussetzung durch das Bundesverfassungsgericht.[172]

Darüber hinaus könnte man erwägen, ob die Bundesregierung durch Abschluss des MoA den USA sogar partiell deutsche Hoheitsgewalt übertrugen im Sinne dieser engen BVerfG-Auslegung: nämlich indem der NSA aufgrund des MoA gestattet wurde, de facto unkontrolliert eigene Selektoren in die hiesige TK-Überwachung einzuspeisen, den BND anwenden zu lassen und die so gewonnenen Erkenntnisse – mutmaßlich ebenso unkontrolliert über ihr Wiesbadener „European Technical Center" – auszuleiten und zu nutzen.

bbb) Das MoA als Bundesgesetz-inhaltlicher Vertrag

Daneben bezieht sich das MoA auch auf Gegenstände der Bundesgesetzgebung im Sinne des Art. 59 Abs. 2 S. 1 Alternative 2 GG. Denn das MoA hatte seit jeher u. a. die vorgenannten Praktiken zum Ziel und Gegenstand, darüber hinaus – wie oben dargelegt – auch den intendierten und durchgeführten Datenzugriff auf den Frankfurter Netzknoten der *Deutschen Telekom AG*. Diese kooperative Erfassung und Verarbeitung jener Daten durch BND und NSA hätte aber real nach deutschem Recht jeweils

---

171) Vgl. nur *Maunz/Dürig/Nettesheim*, 78. Ergänzungslieferung September 2016, GG Art. 59, Rn. 101 mwN; *Pieper* in BeckOK GG/*Pieper*, [32. Ed. 1. März 2015], GG Art. 59, Rn. 31.1; kritisch auch das Minderheitsvotum von gleich vier Verfassungsrichtern in BVerfGE 90, 286 unter C.III.4, http://www.servat.unibe.ch/dfr/bv090286.html dort Rn. 298.

172) BVerfGE 1, 372 (381) vom 29.7.1952; BVerfGE 90, 286 (359), http://www.servat.unibe.ch/dfr/bv090286.html; immerhin rechnet auch das BVerfG eine Fülle von Vertragstypen zu solch politischen Verträgen: Zu politischen Verträgen in diesem Sinne werden insbesondere Bündnisse, Garantiepakte, Abkommen über politische Zusammenarbeit, Friedens-, Nichtangriffs-, Neutralitäts- und Abrüstungsverträge, Schiedsverträge, Grenzverträge sowie Verträge über den Verzicht auf die Ausübung oder die Übertragung von Hoheitsgewalt, ja sogar Doppelbesteuerungsabkommen; vgl. Nachweise und Überblick bei *Maunz/Dürig/Nettesheim*, 78. Ergänzungslieferung September 2016, GG Art. 59, Rn. 99 sowie *Pieper* in BeckOK GG/*Pieper*, [32. Ed. 1. März 2015], GG Art. 59, Rn. 31.

verfassungsfester gesetzlicher Aufgaben- und Befugnisnormen bedurft. Diese bestanden jedoch zumindest bei Unterzeichnung und Durchführung des MoA ab 2002 nicht.[173] Dies hat auch die Bundesregierung offenbar erkannt und eingeräumt durch die entsprechende – allerdings misslungene und immer noch verfassungswidrige[174] – Novellierung des BND-Gesetzes erst zum Ende 2016.

bb) Fazit: BND und NSA kooperierten ohne formell wirksame Grundlage

Politisch ist die Unterlassung der Bundesregierung, eine entsprechende Befassung und Entscheidungsmöglichkeit des Bundestages über das MoA vermieden zu haben, nachdrücklich zu kritisieren. Dies umso mehr, als auch in den Folgejahren eine gehörige Unterrichtung des Bundestages über die praktische Anwendung des MoA unterblieb.

2. EIKONAL: Eine Chronik

Die Operation EIKONAL war ein Kooperationsprojekt zwischen dem BND und der NSA von ca. 2001/2002 bis Mitte 2008 für einen Abgriff von Telekommunikationsdaten an einem Frankfurter Netzknoten [redacted] Die US-Seite hat die Technik geliefert. Im Gegenzug beteiligte der BND die NSA an den Daten aus dem Abgriff. Ziel sollen vorgeblich reine Auslandsverkehre gewesen sein. Die Daten wurden in einer gemeinsamen Arbeitseinheit (Joint SIGINT Activity – JSA) in der BND-Außenstelle Bad Aibling verarbeitet.

[redacted] Die G 10-Kommission und das Parlamentarische Kontrollgremium sind über diese Operation vor Einrichtung des Untersuchungsausschusses im Jahr 2014 nicht unterrichtet worden.

---

173) Vgl. nur das Gutachten *Prof. Papier* (NVwZ Extra 16/2016 und in https://netzpolitik.org/2016/ex-praesident-des-bundesverfassungsgerichts-bnd-zugriff-auf-internet-knoten-wie-de-cix-ist-insgesamt-rechtswidrig/); sowie die Sachverständigengutachten von *Hoffmann-Riem*, MAT A SV-2/1neu; *Papier*, MAT A SV-2/2; *Bäcker*, MAT A SV-2/3.

174) Vgl. die Kritik der Sachverständigen auf der Anhörung im Bundestag im September 2016: https://www.heise.de/newsticker/meldung/Geheimakte-BND-NSA-Ansaetze-fuer-eine-demokratische-Geheimdienstkontrolle-3703988.html?artikelseite=all.

Die Operation EIKONAL wurde angeblich wegen technischer Probleme mit den Filtersystemen im Sommer 2008 eingestellt. Diese Filter sollten dafür sorgen, dass der NSA keine Telekommunikationsdaten von Deutschen zufließen. Tatsächlich wuchs EIKONAL dem BND über den Kopf: Nichtbeherrschbare Technik aber auch ein US-Geheimdienst, der seine überlegenen Fähigkeiten auch gegen den eigenen Kooperationspartner einzusetzen gedachte.

Die Chronik im Folgenden gibt zunächst einen Überblick über den Ablauf der Operation EIKONAL, bevor im Anschluss die zahlreichen rechtlichen, technischen und politischen Risiken bewertet werden, die BND, Kanzleramt, aber auch der Netzbetreiber sehenden Auges eingegangen sind.

Datum	Ereignis
1997	Überlegungen zur Ausweitung der strategischen Kooperation zwischen NSA und BND
14. Juli 1999	BVerfG-Urteil zur strategischen Fernmeldeaufklärung (G 10-Urteil)
2000	NSA äußert gegenüber dem BND Interesse an Zugang zu europäischen Glasfasernetzen in Deutschland
2001	
Mai 2001	Festlegung des Namens EIKONAL für eine Kooperation BND-NSA
26. Juni 2001	Novellierung des Artikel 10-Gesetzes tritt in Kraft: Ausweitung der strategischen FmA des BND auf die internationale Telekommunikation, die leitungsgebunden übertragen wird; vorher – außer zur Abwehr eines bewaffneten Angriffs auf die Bundesrepublik Deutschland – nur Überwachung der Satellitenkommunikation zulässig.
Juli 2001	Verhandlungen des BND mit der NSA über Zukunft der Abhörstation in Bad Aibling (MAT A BND-18a_4, Bl. 19, VS-NfD)
11. Juli 2001	EP veröffentlicht Bericht zum Abhörsystem „Echelon“
24. Juli 2001	Aus Präsidentenrunde zum Thema Bad Aibling: „BK hat keine Bedenken gegen eine Zusammenarbeit mit US-Seite, bei voller Kontrolle durch den BND, voller Transparenz und Beachtung deutschen Rechts durch US-Seite.“[175]
August 2001	Erster Entwurf für Memorandum (MoU/MoA) über Zusammenarbeit BND-NSA in Bad Aibling
11. September 2001	Anschläge von *Al-Kaida* in den USA

175) MAT A BND-18a_4, Bl. 22, VS-NfD; Steinmeier, Protokoll-Nr. 91 I, S. 37.

Datum	Ereignis
12. September 2001	Regierungserklärung von Bundeskanzler *Schröder*: Zusicherung der uneingeschränkten Solidarität Deutschlands mit den USA
7. Oktober 2001	Beginn der „Operation Enduring Freedom“ in Afghanistan (ISAF-Einsatz)
2002	
Januar 2002	Erörterungen im BND über rechtliche und politische Problematiken einer erweiterten Zusammenarbeit mit der NSA in Bad Aibling.
22. März 2002	BND erwähnt in Leitungsvorlage gegenüber Präsidenten, dass bei Kooperation auch ein Kabelabgriff angedacht ist; Erörterung der politischen und rechtlichen Risiken.
19. April 2002	Leitungskonferenz im BND mit Präsident zur strategischen Kooperation mit NSA; u.a. Erörterung der Risiken.
28. April 2002	Unterzeichnung des MoA über die Zusammenarbeit des BND mit der NSA in Bad Aibling durch BND-Pr *Hanning* und NSA-Direktor *Hayden*.
Sommer 2002	[redacted]
2003	
Frühjahr 2003	[redacted]
August 2003	[redacted]
Oktober 2003	BND wendet sich an BKAmt wegen Bestätigungsschreiben für Telekom
November 2003	[redacted]
30. Dezember 2003	[redacted]
2004	
Januar 2004	[redacted]

Datum	Ereignis
Januar 2004	BND (Unterabteilungsleiterebene) empfiehlt mit Nachdruck wegen der grundgesetzlichen Problematik Einbeziehung der G 10-Kommission. Stab der Abt. 2 sieht keine Geltung von Art. 10 GG für sog. Routineverkehre nach Trennung von G 10-Verkehren.
1. März 2004	[redacted]
April 2004	BND erörtert verschiedene Rechtsauffassungen zur Zulässigkeit der Ausleitung von Auslands-Auslands-Verkehren aus G 10-Maßnahmen; Differenzen bestehen auch zwischen BKAmt (Arbeitsebene) und BND
27. April 2004	Erörterung der Rechtsauffassungen am Rande der Präsidentenrunde im BKAmt zwischen BND-Pr (Hanning) und BKAmt/AL6 (Uhrlau)
10. Mai 2004	RegTP genehmigt Erfassungssystem (Einsatz bei EIKONAL)
Juni 2004	Beginn des Abgriffs von leitungsvermittelten Verkehren (Telefonie) in Frankfurt/Main ohne G 10-Anordnung
Juli 2004	[redacted]
August/September 2004	BND erörtert intern erneut die rechtliche Problematik der Ausleitung von Ausland-Ausland-Verkehren aus einer G 10-Erfassung. Ergebnis: BND-Rechtsabteilung und Präsident halten Ausleitung für zulässig
20. Oktober 2004	Besprechung im BKAmt zwischen BND und Abt. 6 unter Leitung von AL6 (Uhrlau): Rechtsfrage wird nicht mehr erörtert; ausgeschlossen werden die Erstellung eines Gutachtes aus dem BKAmt und die Herbeiführung eines förmlichen Beschlusses der G 10-Kommission. Beschlossen wird ein „Probeantrag" für eine G 10-Anordnung zur Ausleitung paketvermittelter Verkehre.[176]
2005	
Januar 2005	Hardware für DAFIS-Filter wird in Bad Aibling aufgebaut und getestet
Frühjahr 2005	„Wirkbetrieb" bei EIKONAL für Telefonie beginnt mit nur noch automatisierter Filterung
27. Mai 2005	Bundesregierung legt Gesetzentwurf zur Änderung des Artikel 10-Gesetz vor (u.a. Einfügung von § 7a G 10 – Übermittlung von G 10-Daten an ausländische öffentliche Stellen); tritt am 5. August 2009 in Kraft
Juni/Juli 2005	Separator zur Trennung der TK-Verkehre in G 10 und Ausland-Ausland in Betrieb

176) MAT A BND-17/3_Auszug_offen, Bl. 11-13.

Datum	Ereignis
Oktober 2005	BSI-"Zertifizierung" des Separators und eines „Verarbeitungssystems" für geplanten Einsatz in Frankfurt/Main
20. Oktober 2005	G 10-Kommission genehmigt G 10-Anordnung zur Ausleitung paketvermittelter Verkehre; Anordnung ist „Türöffner" für die Ausleitung von Ausland-Ausland-Verkehren, die für die Operation EIKONAL genutzt werden sollen.
November 2005	[redacted]
22. November 2005	*Thomas de Maizière* wird Chef des BKAmtes (Beauftragter für die Nachrichtendienste des Bundes) und löst *Frank-Walter Steinmeier* (seit Juli 1999) ab.
1. Dezember 2005	*Ernst Uhrlau* wird BND-Pr (vormals BKAmt/AL6, Geheimdienstkoordinator) *August Hanning* (ehem. BND-Pr) wird StS BMI *Klaus-Dieter Fritsche* wird AL6/Geheimdienstkoordinator im BKAmt
2006	
Januar 2006	Beginn der Übermittlung von Rohdaten aus paketvermittelten TK-Verkehren (IP-Verkehre) an JSA
Ende Januar 2006	Vorfall der in Bad Aibling durch NSA gesteuerten Selektoren *EADS* und *Eurocopter* wird im BND thematisiert
26. Januar 2006	In Vorlage für BND-Pr *Uhrlau* aus Abt. 2 wird über EIKONAL und ausführlich über die Risiken unterrichtet.
Februar 2006	Einsatz eines „Kontrollsystems" bei EIKONAL (für Telefonie) zur Überwachung der ausgeleiteten Verkehre ohne Wissen der JSA in Bad Aibling
Oktober 2006	Gegenüber der G 10-Kommission wird die Spam-Problematik angesprochen; zur G 10-Filter-Problematik kein Wort
2007	
Januar 2007	[redacted]
Mitte Februar 2007	AL2 (*Urmann*) richtet im BND zwei Projektgruppen ein: 1. Dokumentation EIKONAL („Schwachstellenbericht") 2. Verbesserung der G 10-Filterung durch den Separator
Ende März 2007	Vorlage der Ergebnisse der Projektgruppe Separator
Juni 2007	Bislang geringer Output für JSA, Filterprobleme [redacted]; Verquickung mit G 10-Maßnahme wird als Fehler gesehen
Mitte Juni 2007	Einbruch der ausgeleiteten Datenmenge durch Umrouting des Providers
Juli 2007	Vorlage des BND für AL2 (*Urmann*) mit Strategieempfehlung für EIKONAL: Erweiterung oder Beendigung

Datum	Ereignis
August 2007	Vorlage der Dokumentation zu EIKONAL („Schwachstellenbericht“) mit Auflistung von mehr als einem Dutzend z.T. verheerender Schwachstellen bzgl. G 10-Schutz
August/September 2007	Der NSA sollen wegen G 10-Filter-Problemen Daten aus einem außereuropäischen Abgriff angeboten werden.
Mitte/Ende 2007	„Wirkbetrieb“ für IP-Verkehre mit Weiterleitung der Daten an die JSA beginnt
Dezember 2007	BND stellt fest: 100-prozentige Ausfilterung von G 10-geschützter Telekommunikation auch mittelfristig nicht machbar; ein rechtlicher Spielraum mit Fehlertoleranz sei nicht gegeben.
4. Dezember 2007	Besuch von DNI *McConnell* bei ChefBK *de Maizière*: US-Seite bietet dem BND erweiterte Kooperation bei Kabelerfassung an. BND sieht das Angebot kritisch und rät ab.
2008	
Ende Mai 2008	Operation EIKONAL wird eingestellt
Anfang August 2008	BND teilt BKAmt die Einstellung der Operation EIKONAL schriftlich mit.

3. EIKONAL: Abgriff ohne G 10-Anordnung

[redacted]

a) Hintergründe

aa) Freibrief, Transitvertrag, Ausleitung

[redacted]

[redacted]

[redacted]

> [redacted]

> [redacted]

[redacted] 80

177) *S. L.,* Protokoll-Nr. 26 I, S. 65 f.

178) *S. L.,* Protokoll-Nr. 26 I, S. 67.

179) *S. L.*, Protokoll-Nr. 26 I, S. 29.

180) *Dr. Köbele,* Protokoll-Nr. 33 I, S. 143.

bb) Datenströme

[redacted]

cc) Rechtsgrundlagen

Rechtlich brauchen der BND und auch [redacted] jeweils eigene Rechtsgrundlagen für das Eingehen der Zusammenarbeit. Maßgebliche Gesetze sind insbesondere Artikel 10-Gesetz, Telekommunikationsgesetz (TKG) und Bundesdatenschutzgesetz (BDSG). Da sich die Kund_innen eines Telekommunikationsunternehmens regelmäßig nicht mit der Übermittlung ihrer Kommunikationsdaten an Dritte, insbesondere an Geheimdienste, einverstanden erklärt haben und sie regelmäßig keine Kenntnis davon erlangen, stellt das Abgreifen und Ausleiten von Telekommunikationsverkehren einen Grundrechtseingriff dar, der in jedem Einzelfall spezialgesetzlich gerechtfertigt sein muss. Hierfür sehen das Artikel 10-Gesetz für den BND und das TKG i. V. m. mit der

181) *Dr. Köbele,* Protokoll-Nr. 33 I, S. 143.

TKÜV für die Telekommunikationsanbieter jeweils bereichsspezifische Ermächtigungsgrundlagen vor.

b) Abgriff durch den BND

[redacted]

[redacted]

[redacted]

182) § 1 BNDG in der Fassung vom 20. Dezember 1990; § 2 BNDG in den Fassungen vom 9. Januar 2002 und vom 5. Januar 2007.

183) *Hans-Jürgen Papier*, Beschränkungen der Telekommunikationsfreiheit durch den BND an Datenaustauschpunkten, NVwZ – Extra 15/2016, S. 1 (6), abrufbar unter http://rsw.beck.de/rsw/upload/NVwZ/NVwZ-Extra_2016_15.pdf.

> [redacted]

[redacted]

> [redacted]

[redacted]

> [redacted]“[187]

aa) Abgriff in Frankfurt am Main

aaa) BND-Räume bei [redacted]

[redacted]

---

184) *Breitfelder*, Protokoll-Nr. 28 I, S. 78, vgl. auch S. 65.

185) *A. S.,* Protokoll-Nr. 33 I, S. 70.; an anderer Stelle beschrieb er, dass vor dem Projekt EIKONAL zwei weitere leitungsvermittelte Systeme für kabelgestützte Projekte vom BSI zertifiziert wurden; vgl. S. 97.

186) *S. L.,* Protokoll-Nr. 26 I, S. 21; Protokoll-Nr. 26 II – Auszug offen, S. 12.

187) *Dr. Burbaum*, Protokoll-Nr. 24 II – Auszug offen, S. 5.

[redacted]

> [redacted]

[redacted]

> [redacted]

[redacted][191]

bbb) Überwachung mit US-Geräten

Die BND-Zeugen *S. L.* und *A. S.* waren als technische Projektleiter von EIKONAL auch verantwortlich für die Einrichtung des Erfassungskopfes in Frankfurt.[192] Sie wurden nach eigenen Aussagen von zwei BND-Technikern aus Bad Aibling unterstützt.[193]*A. S.* sprach von drei verschiedenen Hardware-Systemen, die am Frankfurter Knoten zur Erfassung von Fax und Telefonie sowie paketvermittelten Verkehren eingesetzt waren.

---

188) *S. L.,* Protokoll-Nr. 26 I, S. 51.

189) *S. L.*, Protokoll-Nr. 26 I, S. 52.

190) *S. L.*, Protokoll-Nr. 26 I, S. 24 f.

191) *S. L.,* Protokoll-Nr. 26 I, S. 39.

192) *S. L.*, Protokoll- Nr. 26 I, S. 69; *A. S.*, Protokoll-Nr. 33 I, S. 84.

193) *S. L.*, Protokoll- Nr. 26 I, S. 21.

Die Details sind eingestuft. Befragt nach der Art der Überwachung, gab der Zeuge *A. S.* folgende Auskünfte:

> „[…] es geht immer darum, Telefon- oder Faxverkehre zu erfassen. […] – – Inhalt, ja. – – Natürlich sind da auch Metadaten dabei, weil ohne die Metadaten können Sie damit nichts anfangen. Wenn Sie Telefongespräche haben und nicht wissen, wer das geführt hat, können Sie das wegwerfen.“[194]

Abgegriffene Signale wurden technisch durch eingekaufte (sogenannte kommerzielle) Multiplexer verstärkt.

> „Dort wird es [das Kabel] erst zunächst in einen Multiplexer eingesteckt. Der Multiplexer ist ein Gerät, was das Signal technisch aufbereitet, und zwar technisch so aufbereitet, dass wir das dann hinterher sozusagen in einen Rechner schieben können.“[195]

Auch US-amerikanische Technik wurde verbaut.[196]

> „In der leitungsvermittelten Erfassung wurde ganz am Anfang des Erfassungszweiges ein US-Gerät eingesetzt. […] Die Hardware musste über verschiedene Adapterlösungen kompatibel gemacht werden. Wir haben das gemacht. Sozusagen der Output dieser speziellen Hardware ging dann wieder in kommerzielle Geräte. Das war nicht Plug and Play, aber mit entsprechender Konfiguration machbar. […] Das waren Lösungen, die zum Teil ich selbst konzipiert und aufgebaut habe, die auf kommerzieller Hardware beruhen, allerdings spezieller Telekommunikationshardware.“[197]

---

194) *A. S.*, Protokoll-Nr. 33 II – Auszug offen, S. 7.

195) *S. L.*, Protokoll-Nr. 26 I, S. 10.

196) *A. S.*, Protokoll-Nr. 33 II – Auszug offen, S. 3, 10 f.

197) *S. L.*, Protokoll-Nr. 26 I, S. 33.

Dass auch die Zeug_innen nicht wussten, welche Technik sie eigentlich verbauten, belegt die Aussage von *A. S.*:

> „Ich habe mir das System selber angeschaut. Das heißt, ich habe Teile davon auseinandergenommen und da reingeschaut, was da drinsteckt. Also, ich kann nicht hundertprozentig sagen, dass da irgendeine Technik drinsteckte, die etwas macht, was wir nicht kontrollieren können. Aber ich bin mal davon ausgegangen, dass die Mitarbeiter in Bad Aibling, die ja mit den Amerikanern dort Zusammenarbeiten, das durchaus beurteilen, was da am Ende rauskommt und was die Amerikaner damit machen.“[198]

ccc) Streckenwahl und Datenströme

Der Datenstrom im Telefonie/Fax-Bereich, der in die Räumlichkeiten des BND floss, umfasste nach Aussagen von *A. S.* ungefähr 622 Megabit.[199] Die Auswahl entsprechender Strecken erfolgte laut *W. K.,* Unterabteilungsleiter im BND, mittels Hard- und Software in der Abteilung 2.[200]

> „Sie müssen überlegen, wo die Kommunikation läuft, an der sie interessiert sind. Sie brauchen Menschen, die natürlich im Vorfeld gucken: Wie sieht die Telekommunikation in dem Zielgebiet aus, in der Region, die Sie interessiert? Wer sind die möglichen Satellitenbetreiber oder Netzbetreiber? Wo macht es Sinn, anzusetzen?“[201]

Er bezeugte, dass „natürlich“ mehrere Strecken angezapft wurden.[202] S. L. unterstrich, dass auch die NSA Interessen bezüglich der Streckenauswahl einbrachte:

---

198) *A. S.*, Protokoll-Nr. 33 II – Auszug offen, S. 12.

199) *A. S.,* Protokoll-Nr. 33 I, S. 99.

200) *W. K.*, Protokoll-Nr. 22 I, S. 29 ff.

201) *W. K.*, Protokoll-Nr. 22 I, S. 29.

202) *W. K.*, Protokoll-Nr. 22 I, S. 59.

> „Für den leitungsvermittelten Verkehr, die Ausland-Ausland-Strecken, hatte die [*NSA*] eine Wunschliste von Ländern, die in ihrem generellen Aufklärungsziel lagen. Die hat sie uns benannt.“[203]

Dabei war der BND auf eine Zusammenarbeit mit dem TK-Betreiber angewiesen.[204] Zu diesem Zweck wurden gesondert Daten in verschiedenen Verfahren erhoben, über deren weitere Verwendung nichts bekannt ist. Der BND führte in diesem Rahmen mittels besonderer Geräte sogenannte Snapshots durch. *S. L.* erklärte dazu:

> „Snapshots nennt man einen kurzen Schnappschuss dessen, was auf der Leitung ist.“[205]

Dabei handelt es sich um kurze Vollerfassungen der Rohdaten einzelner Leitungen, die ohne Reduktion durch Selektion abgegriffen werden. Die Daten wurden dann in der gemeinsamen Arbeitseinheit von NSA und BND, *Joint Sigint Activity*, in Bad Aibling bearbeitet. Eine genauere zeitliche Einordnung ihrer Durchführungen war auf Grundlage der vor dem Ausschuss gemachten Angaben nicht möglich. Eine rechtliche Zulässigkeit der Snapshots war zum damaligen Zeitpunkt nicht ersichtlich. Jedenfalls in der Übergangszeit scheint es sich aber um eine gängige Praxis gehandelt zu haben. So auch der Zeuge *W. K.*:

> „Das war für uns ein völlig normaler Vorgang.“ [206]

bb) Fernmeldegeheimnis als verfassungsrechtlicher Maßstab

Das Grundgesetz schützt in Art. 10 Abs. 1 GG das Fernmeldegeheimnis und stellt dem Gesetzgeber in Art. 10 Abs. 2 GG die Auflage, Eingriffe nur auf Grundlage von Gesetzen vorzunehmen. Es schützt die Telekommunikation, also den vertraulichen Austausch auf Distanz, insbesondere vor staatlicher Kenntnisnahme als Voraussetzung

203) *S. L.*, Protokoll-Nr. 26 I, S. 60, weitere Details sind eingestuft.

204) Vgl. *Dr. Burbaum*, Protokoll-Nr. 24 II – Auszug offen, S. 14; *W. K.,* Protokoll-Nr. 22 I, S. 64.

205) *S. L.*, Protokoll-Nr. 26 II – Auszug offen, S. 7; für nähere Details siehe: Feststellungsteil F.IV.5.a)bb).

206) *W. K.*, Protokoll-Nr. 35 II – Auszug offen, S.47.

für eine freie Entfaltung der Persönlichkeit.[207] Sowohl Inhalte als auch nähere Umstände der Kommunikation fallen darunter.[208] Der Schutzbereich hat eine personelle, sachliche sowie räumliche Dimension.

BND-Mitarbeiter_innen argumentierten vor dem Ausschuss auf unterschiedliche Weise, dass die Abgriffe in Frankfurt, aber auch außerhalb Deutschlands nicht unter den Schutzbereich des Art. 10 GG fielen, solange sie sich nicht auf Staatsbürger_innen oder deutsche Anschlüsse bezögen. Eine Mindermeinung in der Literatur, die vor allem aus dem BND selbst stammt, stimmt dem zu, da der Abgriffsort von technischen und organisatorischen Zufällen bestimmt sei. Sie knüpften stattdessen an den Aufenthaltsort der Gesprächspartner_innen an. Behördenhandeln im Ausland stelle schon gar kein Staatshandeln dar; dagegen könne deswegen keine Abwehr mittels Grundrechten erfolgen. Außerdem sei der Schutzauftrag gegenüber Nicht-Deutschen im Ausland im Vergleich zu Staatsbürger_innen vermindert, beziehungsweise aufgrund der Souveränität ausländischer Staaten „aus rechtlicher Sicht nicht zwingend und aus politischen Gründen gar nicht angeraten."[209] Die Sachverständigen sahen das anders. Aufgrund des Inlandsbezugs eines deutschen Standorts ist eine umfassende Grundrechtsbindung der handelnden Behörde unbestritten.

---

207) Vgl. BVerfGE 100, 313-403, https://www.bverfg.de/e/rs19990714_1bvr222694.html, dort Rn. 162; BVerfGE 115, 166-204, https://www.bverfg.de/e/rs20060302_2bvr209904.html, dort Rn. 65 ff.

208) Vgl. BVerfGE 100, 313-403, https://www.bverfg.de/e/rs19990714_1bvr222694.html, dort Rn. 161; BVerfGE 115, 166-204, https://www.bverfg.de/e/rs20060302_2bvr209904.html, dort Rn. 70 f.

209) *D. Kreuter/A. K. Möbius*, Verfassungsrechtliche Vorgaben für nachrichtendienstliches Handeln im Ausland: Extraterritoriale Geltung der Grundrechte? In: BWV Heft 7 Juli 2009., S. 146 ff.; vgl. *A. F.,* Protokoll-Nr. 41 I, S. 105; *Graulich*, MAT A SV-11/2, S. 63; *Wilfried Karl/Michael Soiné*, Neue Rechtsgrundlagen für die Ausland-Ausland-Fernmeldeaufklärung, in: NJW 2017, S. 919; die Autoren sind Beamte des BND, ihr Beitrag gründet auf persönlichen Auffassungen; unter der Bezeichnung ‚Theorie des virtuellen Auslands' ist im Ausschuss ein plakatives Bild entstanden, kabelgebundene Überwachung außerhalb des Geltungsbereichs der Rechtsordnung zu verorten.; ob dies so umgesetzt wurde, blieb im Ausschuss offen; vgl. Abgeordneter *Christian Flisek,* Protokoll-Nr. 28 I, S. 66; *Breitfelder* greift das Konzept auf S. 84 auf; Kritik des „Abhörens des offenen Himmels" schon bei *Berthold Huber,* Die strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefugnisse und Regelungsdefizite, in: NJW 2013, S. 2572 (2575).

aaa) Umfassende Grundrechtsbindung

Richtigerweise nahmen die Sachverständigen einen umfassenden Schutz des Fernmeldegeheimnisses an, der territorial nicht beschränkt ist.[210] Der Wortlaut Art. 10 Abs. 1 GG beschränkt den räumlichen Schutzbereich des Fernmeldegeheimnisses nicht. Das BVerfG hat im G 10-Urteil von 1999 klar festgestellt:

> „Der räumliche Schutzumfang des Fernmeldegeheimnisses ist nicht auf das Inland beschränkt.“[211]

BND-Zeug_innen suchten sich die Lücken, die der Gesetzgeber bei den Gesetzesnovellen 2001 (und 2006) hinterließ, als er bewusst auf eine Regelung der Auslands-Auslandsverkehre verzichtete. Sie zogen auch die Entscheidung des Bundesverfassungsgerichts (BVerfG) zum Artikel 10-Gesetz aus dem Jahr 1999 heran, um aufzuzeigen, dass dem BND hierin die Möglichkeit der grundrechtsfreien Auslandserfassung explizit offen gehalten worden wäre. Diese Auffassung sollte ihre Legitimität wiederum aus der geübten Praxis schöpfen:

> „Das Urteil des Bundesverfassungsgerichts von 1999 sagt dazu: Es bedarf hier keiner Entscheidung über den Grundrechtsschutz des Ausländers im Ausland. […] Das hat es offengelassen, natürlich. Das ist eine Auslegungsfrage. […] Na ja, es hätte ja die Gelegenheit gehabt, es anders zu entscheiden.“[212]

Diese Frage war auch nach Aussagen von Herrn *Papier*, der damals als Richter an der Entscheidung beteiligt war, gar nicht entscheidungsrelevant in dem besagten Urteil.[213] Bezüglich des nicht-deutschen Klägers im Ausland mangelte es ihm in seiner

---

210) Eine umfassende Grundrechtsbindung ist in der Fachliteratur herrschende Meinung. Anders *Graulich*, MAT A 11/2, S. 49 f, der bemerkenswerterweise den personellen Schutzbereich nicht als Menschenrecht geprüft hat und stattdessen den räumlichen Schutzbereich in einer eigenwilligen Theorie vom normgeprägten Grundrecht sucht, die vor dem Hintergrund der Grundrechtsbindung nach Art. 1 Abs. 3 GG und der Konstruktion von Art. 10 GG als Abwehrgrundrecht nicht zu überzeugen vermag.

211) BVerfGE 100, 313, https://www.bverfg.de/e/rs19990714_1bvr222694.html, Ls. 2.

212) *Dr. Burbaum*, Protokoll-Nr. 24 I, S. 77.

213) Vgl. *Hans-Jürgen Papier*, Beschränkungen der Telekommunikationsfreiheit durch den BND an Datenaustauschpunkten, NVwZ – Extra 15/2016, S. 1 (11), abrufbar unter http://rsw.beck.de/rsw/upload/NVwZ/NVwZ-Extra_2016_15.pdf; *Bertold*

Gehilfenstellung schon an der eigenen Betroffenheit, er hörte nur den Anrufbeantworter einer anderen Klägerin ab, weswegen seine Klage gar nicht materiell geprüft wurde.[214]

Der Schwerpunkt der Argumentation muss auf der Grundrechtsbindung staatlicher Gewalt nach Art. 1 Abs. 3 GG liegen.[215] Eine Beschränkung im Ausland ist nur für begründete Ausnahmefälle denkbar, in denen die Bundesregierung im Ausland ihre volle Staatssouveränität nicht ausüben kann oder durch internationale Verpflichtungen in ihren Handlungsoptionen eingeschränkt ist. Das ist aber für die Auslandsüberwachung nicht der Fall.216 Völkerrechtliche Normen selbst schützen das Fernmeldegeheimnis.217 Bäcker folgert:

> „Weder das Grundgesetz noch das Völkerrecht hindern den Gesetzgeber generell, die extraterritoriale Tätigkeit deutscher staatlicher Stellen zu regeln. Da Grundrechtseingriffe nur auf formellgesetzlicher Grundlage zulässig sind, ist eine solche Regelung vielmehr sogar verfassungsrechtlich geboten, wenn deutsche Stellen im Ausland in Grundrechte eingreifen sollen."[218]

Huber, Die strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefugnisse und Regelungsdefizite, in: NJW 2013, S. 2572 (2574); die Ausführungen im G 10-Urteil sind inhaltlich als Beschreibung einzuordnen, jedoch innerhalb des Urteils missverständlich platziert und legen damit überschießende Fehlinterpretationen nahe, das Gericht führt jedoch zugleich aus, dass die wiedergegeben BND-Darstellungen seitens der Kläger_innen „nicht substantiiert" infrage gestellt wurden, vgl. BVerfGE 100, 313, https://www.bverfg.de/e/rs19990714_1bvr222694.html, Rn. 230.

214) Vgl. BVerfGE 100, 313, https://www.bverfg.de/e/rs19990714_1bvr222694.html, Rn. 165; *Johannes Caspar*, Strategische Auslandsüberwachung – Jenseits der Grenze des Rechtsstaats?, in: PinG 2014, H. 1, S. 4.

215) Vgl. *Hans-Jürgen Papier*, Beschränkungen der Telekommunikationsfreiheit durch den BND an Datenaustauschpunkten, NVwZ – Extra 15/2016, S. 1 (3), abrufbar unter http://rsw.beck.de/rsw/upload/NVwZ/NVwZ-Extra_2016_15.pdf.

216) Vgl. *Bäcker*, MAT A SV 2/3, S. 20 f*; Johannes Caspar*, Strategische Auslandsüberwachung – Jenseits der Grenze des Rechtsstaats?, in: PinG 2014, H. 1, S. 4. mit weiteren Verweisen; *Bertold Huber*, Die strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefugnisse und Regelungsdefizite, in: NJW 2013, S. 2572 (2575); unabhängig davon ist die Frage der Schutzpflichten.

217) Vgl. *Bäcker*, MAT A SV 2/3, S. 21 f.

218) *Bäcker*, MAT A SV 2/3, S. 22.

bbb) Grundrechtsschutz bei deutschem Abgriffspunkt

Ein Schutz des Fernmeldegeheimnisses ist nach überzeugender Ansicht zumindest dann anzunehmen, wenn ein Inlandsbezug der Maßnahmen besteht. Spätestens wenn Daten im Inland erhoben oder verarbeitet werden, ist nach richtiger Auffassung durch diese territoriale Verknüpfung genügend Anlass für eine volle Grundrechtsbindung gegeben. Einen solchen Bezug hat das Bundesverfassungsgericht (BVerfG), unter Beteiligung von *Papier*, in der G 10-Entscheidung für Satellitenüberwachungsanlagen auf deutschem Gebiet 1999 bejaht, da es „eine technisch-informationelle Beziehung zu den jeweiligen Kommunikationsteilnehmern und ein[en] – den Eigenarten von Daten und Informationen entsprechender – Gebietskontakt hergestellt“ sah.[219] Ein Knotenpunkt lässt sich sehr konkret verorten; der Datenfluss erfolgt durch deutsches Territorium und nicht abgelegenen Luftraum.

> „Setzt der BND für die Überwachung bei einem Kabelende oder einem Netzknoten innerhalb Deutschlands an, so besteht danach ein territorialer Bezug zur Bundesrepublik.“[220]

Nach der für das Recht auf Informationelle Selbstbestimmung entwickelten Dogmatik, die das BVerfG mit dem G 10-Urteil auf Eingriffe in das Fernmeldegeheimnis übertragen hat, bezieht sich bei der Telekommunikationsüberwachung der Eingriff nicht nur auf die Erhebung von Daten, sondern auch auf die weitere Verarbeitung und Übermittlung.[221] Mit dieser Logik mehrstufiger Eingriffe ist nicht singulär auf einen einzelnen Ort innerhalb des Datenflusses abzustellen; vielmehr können mehrere Orte grundrechtlich

---

219) BVerfGE 100, 313-403, https://www.bverfg.de/e/rs19990714_1bvr222694.html, dort Rn. 176; vgl. *Papier*, MAT A SV-2/2, S. 7; *Bertold Huber*, BND-Gesetzreform – gelungen oder nachbesserungswürdig?, in: ZRP 2016, S. 162 (163); *Johannes Caspar*, Strategische Auslandsüberwachung – Jenseits der Grenze des Rechtsstaats?, in: PinG 2014, H. 1, S. 4.

220) *Bäcker*, MAT A SV-2/3., S. 18, vgl. BVerfGE 100, 313-403, https://www.bverfg.de/e/rs19990714_1bvr222694.html, Ls.2, Rn. 190 f.

221) Vgl. BVerfGE 100, 313-403, https://www.bverfg.de/e/rs19990714_1bvr222694.html, Rn. 164; BVerfGE 110, 33 – 76, https://www.bverfg.de/e/fs20040303_1bvf000392.html Rn. 106; BVerfGE 125, 260 (323), http://www.bverfg.de/e/rs20100302_1bvr025608.html, Rn. 191, BVerfGE 130, 151 – 212, https://www.bverfg.de/e/rs20120124_1bvr129905.html, Rn. 169.

relevant werden, wenn an ihnen Erhebungs-, Verarbeitungs- oder sonstige Schritte durchgeführt werden.

Der Wortlaut von Art. 10 Abs. 1 GG hebt mit dem „Fernmeldegeheimnis" die besondere Schutzbedürftigkeit von Kommunikation während einer Übermittlung hervor und stellt eben gerade auf den Transportweg der Daten und dessen spezifische Unsicherheiten ab.[222] Zentral ist die Distanz im Kommunikationsverhältnis, unabhängig davon über welche Leitungen die Verkehre transportiert werden. Sie birgt gerade die spezifische Gefahr einer Datenübermittlung. Bei der rechtlichen Bewertung des Abgriffs ist daher auch auf den Ort des Abgriffs abzustellen. Hier ist der deutsche Betreiber Organisator des Datentransports und Frankfurt Standort der Ausleitung an den BND. Der Standort des Abgriffs ist kein „zufälliges"[223] Kriterium, sondern an rechtliche Gegebenheiten geknüpft. Davon geht auch der BND aus:

> „Im Ausland kann er [der BND] keine deutschen Provider – – – kann er keine Provider verpflichten. Er braucht eigenen technischen Unterbau und Zugang. Damit sieht er sich immensen Herausforderungen im technischen Bereich gegenüber, Vielfalt der verschiedenen Dienste, der Datenmengen."[224]

Der jeweils angesprochene Betreiber ist jedenfalls im Inland an die deutsche Rechtsordnung gebunden. Bei der Ausleitung werden die Datenströme am Frankfurter Knotenpunkt gedoppelt und an einem inländischen Datenaustauschpunkt übergeben. Der BND ist eine im Inland ansässige Behörde und voll grundrechtsgebunden.[225] Es lässt

222) Vgl. LAG Berlin-Brandenburg, NZA-RR 2011, S. 342 (343): „Art. 10 Abs. 1 GG trägt gerade der Besonderheit Rechnung, dass für den Kommunikationsteilnehmer keine technischen Möglichkeiten vorhanden sind, das Entstehen und die Speicherung von Verbindungsdaten durch den Nachrichtenübermittler zu verhindern oder auch nur zu beeinflussen."

223) *D. Kreuter/A. K. Möbius*, Verfassungsrechtliche Vorgaben für nachrichtendienstliches Handeln im Ausland: Extraterritoriale Geltung der Grundrechte? in: BWV HEFT 7 Juli 2009., S. 146 (148).

224) *A. S.,* Protokoll-Nr. 41 I, S. 104.

225) *Bertold Huber*, BND-Gesetzreform – gelungen oder nachbesserungswürdig?, in: ZRP 2016, S. 162 (164); ders., Die strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefugnisse und Regelungsdefizite, in: NJW 2013, S. 2572 (2575).

sich rechtlich keinerlei Begründung dafür finden, die Grundrechtsgeltung innerhalb der Bundesrepublik zu relativieren.

ccc) Dynamischer Grundrechtsschutz – Globalisierung der Kommunikation

Technische Neuerungen haben die Telekommunikationsinfrastruktur grundlegend verändert.

> „Ob bei dem Transportvorgang nur Knotenpunkte in Deutschland passiert werden, steht nicht von vornherein fest und ist jedenfalls für den Nutzer nicht vorhersehbar."[226]

> „Zu beachten ist dabei, dass die Inhalte auch bei einer rein innerdeutschen Kommunikation über das Ausland versandt worden sein können."[227]

Grundrechtsschutz muss dynamisch gefasst werden. Das G 10-Urteil von 1999 ist vor der Gründung von Facebook und der großflächigen Einführung von Voice-over-IP gefällt worden. Mit Blick auf die Digitalisierung hat das BVerfG den Persönlichkeitsschutz mehrmals neu konkretisiert, und die Rechtsprechungslinien lassen sich auf Art. 10 GG übertragen. Das Fernmeldegeheimnis lässt Raum für zeitlich modifizierte Auslegung und muss mit technischen Veränderungen Schritt halten. Davon geht auch der ehemalige Richter *Papier* aus, der 1999 beim Karlsruher G 10-Urteil mitgewirkt hatte.

> „Moderne Technologien erlauben indes auch Zugriffe der deutschen öffentlichen Gewalt auf ausländische Fernmeldeverkehre, selbst mit Überwachungsanlagen, die auf dem Gebiet der Bundesrepublik

226) *Hoffmann-Riem*, MAT A SV-2/1-neu, S. 10, vgl. auch Argumentation eines Beschwerdeführers im G 10-Verfahren 1999, in: BVerfGE 100, 313-403, https://www.bverfg.de/e/rs19990714_1bvr222694.html, Rn. 57.

227) *Bäcker*, MAT A SV-2/3, S. 11.

> Deutschland stationiert sind. Daher stellt sich die Frage nach der territorial-räumlichen Geltungskraft des Grundrechts aus Art. 10 GG mit aller Dringlichkeit.“[228]

Bertold Huber beschrieb ein Festhalten an einer räumlichen Begrenzung als ignorante „überholte verfassungsrechtliche Mehrheitsmeinung des letzten Jahrhunderts“, die den „rechtspolitisch gebotenen Herausforderungen nicht gerecht“ wird.[229] Der Sachverständige *Wolfgang Hoffmann-Riem* verortete den grundrechtlichen Schutzzweck in der menschlichen Entfaltungsfreiheit.

> „Die global organisierte Realität wäre sonst geeignet, den Freiheitsschutz weitgehend auszuhebeln. Deshalb bedarf es auch neuer Ansätze für rechtlichen Schutz. Das Bundesverfassungsgericht hat vielfach anerkannt, dass die Änderung tatsächlicher Umstände Anlass sein kann und muss, die Grundrechte so auszulegen, dass das Niveau des Grundrechtschutzes erhalten bleibt.“[230]

Und daraus folgt:

> „Grundrechtsschutz als Schutz der Entfaltungsfreiheit knüpft an das Verhalten von Grundrechtsträgern an. Danach – – und nicht nach den Zufälligkeiten eines, insbesondere eines von Dritten ohne Einwirkung der Kommunikatoren bestimmten, Transportwegs – richtet sich die Reichweite des Schutzes durch Kommunikations- und Persönlichkeitsgrundrechte.“[231]

Grundrechtsschutz muss sich anpassen:

---

228) Vgl. *Hans-Jürgen Papier*, Beschränkungen der Telekommunikationsfreiheit durch den BND an Datenaustauschpunkten, NVwZ – Extra 15/2016, S. 1 (5), abrufbar unter http://rsw.beck.de/rsw/upload/NVwZ/NVwZ-Extra_2016_15.pdf.

229) *Bertold Huber*, BND-Gesetzreform – gelungen oder nachbesserungswürdig?, in: ZRP 2016, S. 162 (166).

230) *Hoffmann-Riem,* MAT A SV-2/1, S. 4.

231) *Hoffmann-Riem*, MAT A SV-2/1, S. 10.

> „Der Schutz würde teilweise leerlaufen, wenn er davon abhinge, ob ein Kommunikationsvorgang mehr oder minder unvorhersehbar/zufällig über Leitungen in deutschen oder in nichtdeutschen Gebieten abgewickelt wird.“[232]

Telekommunikation hat sich längst losgelöst von seiner Einbettung in ein nationalstaatlich organisiertes Post- und Telefoniewesen.[233] Mit der technischen Entwicklung hat sie sich inzwischen globalisiert und erfordert eine Anpassung der Schutzanforderungen.

cc) Grundrechtseingriff – Ausleitung, Erhebung, Verarbeitung, Übermittlung

Vor dem Ausschuss wurde darüber gestritten, ab welchem Zeitpunkt die Datenabgriffe grundrechtsrelevant werden und ob sich die einzelnen Verarbeitungsschritte unterscheiden lassen. Das ist auch vor dem Hintergrund relevant, als die Streubreite der vom BND gewonnenen Datenmasse mit ihrer fortschreitenden Verarbeitung entsprechend des Auftragsprofils der Bundesregierung verringert wird.

Am Maßstab des Fernmeldegeheimnisses stellt jede Kenntnisnahme, Aufzeichnung und Verwertung von Kommunikationsdaten durch den Staat einen rechtfertigungsbedürftigen Grundrechtseingriff dar.[234] Entsprechend hatte das BVerfG für die nachrichtendienstliche Überwachung schon 1999 klargestellt:

> „Für die Kenntnisnahme von erfaßten Fernmeldevorgängen durch Mitarbeiter des Bundesnachrichtendienstes steht folglich die Eingriffsqualität außer Frage. Aber auch die vorangehenden Arbeitsschritte müssen in ihrem durch den Überwachungs- und Verwendungszweck bestimmten Zusammenhang betrachtet werden.“[235]

---

232) *Hoffmann-Riem*, MAT A SV-2/1, S. 10.

233) Vgl. *Hoffmann-Riem*, MAT A SV-2/1, S. 10.

234) Vgl. BVerfGE 85, 386 – 405, https://www.bverfg.de/e/rs19920325_1bvr143088.html, Rn. 57; BVerfGE 100, 313-403, https://www.bverfg.de/e/rs19990714_1bvr222694.html, Rn. 186.

235) BVerfGE 100, 313-403, https://www.bverfg.de/e/rs19990714_1bvr222694.html, Rn. 186.

Dies beginnt bereits bei der zielgerichteten Abschöpfung des auf einer Leitung befindlichen Datenflusses oder bestimmter Anteile hiervon als eine Beschaffung personenbezogener Daten:

> „Eingriff ist daher schon die Erfassung selbst, insofern sie die Kommunikation für den Bundesnachrichtendienst verfügbar macht und die Basis des nachfolgenden Abgleichs mit den Suchbegriffen bildet.“[236]

Davon geht auch *A. F.* aus:

> „‚ Erfassen‘ bedeutet, soweit ich mich erinnern kann […], die Verfügbarmachung für den Bundesnachrichtendienst, also die theoretische Möglichkeit – – Ich glaube, man kann es runterbrechen auf den ersten Punkt, wo es in die Erfassungsgeräte des Bundesnachrichtendienstes gelangt.“[237]

Zur weiteren mit dem Vorgang des Speicherns beginnenden, stufenweisen Verarbeitung stellte das BVerfG eine sich intensivierende Fortsetzung des Grundrechtseingriffs in Art. 10 GG fest, die ihrerseits einer bereichsspezifischen und angemessenen gesetzlichen Rechtfertigungsgrundlage bedarf:

> „Der Eingriff setzt sich mit der Speicherung der erfaßten Daten fort, durch die das Material aufbewahrt und für den Abgleich mit den Suchbegriffen bereitgehalten wird. Dem Abgleich selbst kommt als Akt der Auswahl für die weitere Auswertung Eingriffscharakter zu. Das gilt unabhängig davon, ob er maschinell vor sich geht oder durch Mitarbeiter des Bundesnachrichtendienstes erfolgt, die zu diesem Zweck den Kommunikationsinhalt zur Kenntnis nehmen. Die weitere Speicherung nach Erfassung und Abgleich ist als Aufbewahrung der Daten zum Zweck der Auswertung gleichfalls Eingriff in Art. 10 GG.“[238]

---

236) BVerfGE 100, 313-403, https://www.bverfg.de/e/rs19990714_1bvr222694.html, Rn. 186.

237) *A. F.,* Protokoll-Nr. 41 I, S. 116 f.

238) BVerfGE 100, 313-403, https://www.bverfg.de/e/rs19990714_1bvr222694.html, Rn. 186.

Schließlich sieht es in der Übermittlung der so gewonnenen personenbezogenen Daten „eine erneute Durchbrechung des Fernmeldegeheimnisses“, „die größere Beeinträchtigungen als der Ersteingriff zur Folge haben kann.“[239]

Dabei bestimmt sich die Intensität der Grundrechtsbeeinträchtigung zum einen aus ihrem klandestinen Charakter unter Umgehung der versprochenen infrastrukturellen Vertraulichkeit der Übertragungswege, was schon im Vorfeld zu einer Befangenheit in der Kommunikation führt und damit über individuelle Beeinträchtigungen hinaus die Kommunikation der Gesellschaft insgesamt berührt.[240] Zum anderen „fällt ins Gewicht, dass jeder Teilnehmer am internationalen Telekommunikationsverkehr den Überwachungsmaßnahmen ausgesetzt ist, ohne daß dies mit seinem Verhalten in irgendeiner Weise in Beziehung gebracht werden könnte oder durch ihn veranlasst wäre.“[241] Schließlich ist bei der Intensität des Grundrechtseingriffs „die fehlende Anonymität der Kommunikationsteilnehmer zu berücksichtigen“.[242]

Danach bleibt festzustellen, dass die Überwachung des Telekommunikationsverkehrs durch die Nachrichtendienste in jeder Stufe von der Erhebung über die Verarbeitung bis hin zur Übermittlung, nicht nur aber insbesondere an nicht-deutsche Stellen, einer gesetzlichen Grundlage bedarf, die den verfassungsrechtlichen Anforderungen des Art. 10 GG entspricht.

aaa) Snapshots & Streckeninformationen als Eingriff

Dies betrifft auch Snapshots und Streckeninformationen.

In Vorbereitung der Transitüberwachung erfolgten bereits im Rahmen der Strecken- und Kabelauswahl sowie zur Einstellung der Erfassungstechnik mehrere Totalerhebungen der auf den betroffenen Leitungen anfallenden Telekommunikationsverkehre

239) BVerfGE 100, 313-403, https://www.bverfg.de/e/rs19990714_1bvr222694.html, Rn. 269.

240) Vgl. BVerfGE 100, 313-403, https://www.bverfg.de/e/rs19990714_1bvr222694.html, Rn. 233.

241) BVerfGE 100, 313-403, https://www.bverfg.de/e/rs19990714_1bvr222694.html, Rn. 231.

242) BVerfGE 100, 313-403, https://www.bverfg.de/e/rs19990714_1bvr222694.html, Rn. 233.

(„Signale“). Dazu kopierte der BND mit einem „Extragerät“ mittels eines sog. Snapshots den vollständigen Leitungsfluss an einem bestimmten Punkt direkt vom Kabel.[243] Die so erhobenen Daten wurden dann von BND und NSA in der JSA in Bad Aibling ausgewertet. Solche, wenn auch nur kurzzeitigen Totalabgriffe sind ihrerseits grundrechtlich als Datenerhebung von erheblichem Gewicht zu qualifizieren, da gleichermaßen Inhalts- wie Metadaten der zum jeweiligen Zeitpunkt laufenden Kommunikation unterschiedslos erfasst werden. Das räumte zumindest grundsätzlich auch der im Ausschuss befragte BND-Mitarbeiter *A. F.* ein:

> „Sie haben damit aufgezeichnete Daten, die unter Umständen Grundrechtsträger betreffen.“[244]

Daran ändert auch die Aussage des ehemaligen, für die technische Aufklärung zuständige Abteilungsleiters 2 im BND, *Dieter Urmann*, gegenüber dem Ausschuss, nichts, dass die Snapshots „in der Regel eher“ dazu gedient hätten, Streckenkennungen und Ähnliches herauszufinden.[245] Denn sie erklärt nicht, wie personenbezogene Daten erhoben und im Hinblick auf die Treffsicherheit des Datenstaubsaugers ausgewertet worden sein sollen, ohne zwischendurch (jedenfalls eine gewisse Zeit lang) gespeichert und damit für die vom BND festgelegten Zwecke „erfasst“ worden zu sein.[246] Die datenschutzrechtlichen Begriffe „Erfassen“ und „Aufnehmen“ (§ 3 Abs. 4 Nr. 1

243) *A. S.*, Protokoll-Nr. 33 I, S. 101.

244) *A. F.,* Protokoll-Nr. 41 I, S. 105.

245) *Dr. Urmann*, Protokoll-Nr. 39 I, S. 14.

246) Dass eine Speicherung stattgefunden hat, ist unbestritten und wird durch die Zeugenaussagen von *S. L.*, Protokoll-Nr. 26 II – Auszug offen, S. 7; *A. S.*, Protokoll-Nr. 33 I, S. 101; *Dr. Urmann*, Protokoll-Nr. 39 I, S. 14 belegt.

BDSG)[247] beschreiben jede Form der Transformation einer Information aus der geistigen oder lebenswirklichen Sphäre in ein speicherbares Medium. Auch die Dauer der Speicherung ist für die Frage der Grundrechtsrelevanz grundsätzlich unmaßgeblich.[248]

bbb) Informationsvorbereitungseingriff

Auch die Fernmeldeaufklärung als „Informationsvorbereitungseingriff" stellt einen Eingriff in das Fernmeldegeheimnis dar. *A. F.* beschrieb den Abgriff der Daten unpassenderweise mit einem Polizeibeamten, der Streife fährt:

> „SIGINT als Streife fahren – vor dem Bundesverwaltungsgericht letztes Jahr fiel dieses Bild, dieser Begriff. Es handelt sich um einen Informationsvorbereitungseingriff."[249]

Das BVerfG nimmt eine grundrechtsrelevante Gefährdung schon dann an, wenn eine Datenerhebung personenbezogene Daten für Behörden verfügbar macht und diese die Basis für einen nachfolgenden Ableich mit Suchkriterien bildet.[250]

> „Maßgeblich ist aber insgesamt, ob sich bei einer Gesamtbetrachtung mit Blick auf den durch den Überwachungs- und Verwendungszweck bestimmten Zusammenhang das behördliche Interesse an den betroffenen Daten bereits derart verdichtet hat, dass ein Betroffensein in

247) In seinem, die Telekommunikationsüberwachung des BND betreffenden Urteil von 1999 legte sich das BVerfG nicht auf die Begrifflichkeiten des BDSG fest; es spricht allgemein von „erlangten Daten" (Erhebung), deren „Erfassung und Aufzeichnung" (Speicherung) sowie „Verwendung" (Verarbeitung im engeren Sinne oder Nutzung), an anderer Stelle heißt es pauschal „Überwachung und Aufzeichnung" (BVerfGE 100, 313-403, https://www.bverfg.de/e/rs19990714_1bvr222694.html, Rn. 186 ff. und 257 ff.).

248) Vgl. allerdings die Einschränkung in BVerfGE 100, 313-403, https://www.bverfg.de/e/rs19990714_1bvr222694.html, Rn. 186.

249) *A. F.*, Protokoll-Nr. 41 I, S.102; vgl. *Breitfelder*, Protokoll-Nr. 28 I, S. 12; die Figur technisch bedingten Miterfassung, die von den Zeugen herangezogen wurde, um die Erfassung für rechtlich belanglos zu erklären, greift schon deswegen nicht, da innerdeutsche Daten schon gar nicht geeignet für eine Maßnahme nach § 5 Artikel 10 Gesetz sind und damit gar keine Basis einer solchen Erfassung darstellen können; vgl. BVerfG, Urteil vom 14. Juli 1999, 1 BvR 2226/14, Rn. 186 f; BVerWG, Urteil vom 28. Mai 2014, A 1.13, Rn. 23.

250) BVerfGE 100, 313 (366 f., 380), https://www.bverfg.de/e/rs19990714_1bvr222694.html; 115, 320 (343), https://www.bverfg.de/e/rs20060404_1bvr051802.ht; 120, 378 (398), https://www.bverfg.de/e/rs20080311_1bvr207405.html.

> einer einen Grundrechtseingriff auslösenden Qualität zu bejahen ist.“[251]

Der von *A. F.* ebenfalls gezogene Vergleich der Selektionspraxis des BND bei der Aufbereitung der durch den Telekommunikationsabgriff gewonnenen Daten mit dem automatisierten Datenabgleich, den die Polizei bei der Kfz-Kennzeichenerfassung vornimmt, geht fehl. Der Totalabgriff von Kommunikationsdaten in einem rechtlich vor unberechtigter Kenntnisnahme besonders geschützten Infrastrukturbereich – wie dies bei der Telekommunikationsüberwachung stattfindet – ist mit der Erfassung eines in der Öffentlichkeit aufgrund gesetzlicher Anordnung zum Zwecke der Identifikation zur Schau getragenen Pkw-Kennzeichens gerade nicht vergleichbar.

ccc) Weitere Eingriffe

Weitere Eingriffe stellen nach dem Stufenmodell des Bundesverfassungsgerichts[252] auch der Datenabgriff mittels Selektion, die Verarbeitung und die Übermittlung der Kommunikationsdaten dar. Gerade auch bei dem Datenabgriff mittels Selektion handelt es sich um einen qualitativ völlig neuen Eingriff, der sich nicht in dem Abgleich mit einer bestehenden Datenbank erschöpft und dessen Suchprofile auch nicht unbedingt auf vorwerfbarem Handeln aufbauen.

dd) Kein rechtfertigendes Gesetz

Dem BND stand keine Befugnis zu, Transitverkehre und ausländische Binnenkommunikation in Frankfurt am Main abzugreifen.[253] Seine Abgriffe, insbesondere von Telefonie- und Fax-Datenströmen, waren rechtswidrig und verstießen gegen das Grundgesetz.

251) BVerfGE 120, 378-433, https://www.bverfg.de/e/rs20080311_1bvr207405.html, Rn. 65 mit Verweis auf BVerfGE 115, 320 (343), https://www.bverfg.de/e/rs20060404_1bvr051802.ht.

252) BVerfGE 100, 313-403, https://www.bverfg.de/e/rs19990714_1bvr222694.html, Rn. 186.

253) *Bertold Huber*, Die strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefugnisse und Regelungsdefizite, in: NJW 2013, S. 2572 (2576); *Papier*, MAT A SV-2/2, S. 14; zu § 1 BNDG *Bäcker*, MAT A SV-2/3, S. 16.

aaa) BND auf Abwegen

Unter den Stichworten „Transit“ und „Routine“, beides Bezeichnungen für Kommunikationsverbindungen mit den Endpunkten im Ausland – also ausländische Binnenkommunikation oder internationale Ausland-Ausland-Verkehre, überwachte der BND massenhaft Datenströme ohne ausreichende Rechtsgrundlage. [254] Im BND wurde die „Routine“-Kategorie als vermeintlicher Gegenbegriff zu sogenannten G-10-Verkehren gehandelt. Eben diese Verbindungen waren besonders wichtig für den Geheimdienst. *Bertold Huber* sowie *Hans-Jürgen Papier* bezeichneten die Routineverkehre als das „Kerngeschäft“ des Geheimdienstes.[255] *Ernst Uhrlau*, damals Abteilungsleiter 6 im Bundeskanzleramt und später Präsident des BND:

> „Routineverkehre sind für den BND vielfach sehr viel relevanter als die eingegrenzten G-10-Erfassungen, weil die Routineverkehre das breitere Auftrags- und Interessenprofil der Bundesregierung berühren.“[256]

Mitarbeiter_innen des BND stützten deren Abgriff gegenüber dem Ausschuss auf die allgemeine Aufgabenbeschreibung sowie die Generalbefugnis im damaligen BND-Gesetz und damit auf pauschale Regelungen ohne viel Gehalt. Demgegenüber war die anlasslose und umfassende Überwachung von Auslandsverkehren zum damaligen Zeitpunkt mit § 5 Artikel-10-Gesetz abschließend geregelt.[257] In der von der Bundesregierung abgesegneten Praxis des BND spielte diese Regelung jedoch keine Rolle

254) Vgl. Dr. *Burbaum*, Protokoll-Nr. 24 I, S. 28.

255) *Bertold Huber*, Die strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefugnisse und Regelungsdefizite, in: NJW 2013, S. 2572 (2575)*; Hans-Jürgen Papier*, Beschränkungen der Telekommunikationsfreiheit durch den BND an Datenaustauschpunkten, in: NVwZ – Extra 15/2016, S. 1 (6).

256) *Uhrlau*, Protokoll-Nr. 53 I, S. 39.

257) In der Fassung vom 26. Juni 2001; die Frage, ob sich Ausland-Ausland-Verkehre unter § 5 überhaupt fassen lassen, ist davon unabhängig; Ausführungen zur Verfassungswidrigkeit von § 5 Abs. 2 Artikel 10-Gesetz wegen Verletzung des Gleichheitssatzes aus Art. 3 Abs. 1 GG bei *Berthold Huber*, Die strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefugnisse und Regelungsdefizite, in: NJW 2013, S. 2572 (2574); sowie *bei Hans-Jürgen Papier*, , Beschränkungen der Telekommunikationsfreiheit durch den BND an Datenaustauschpunkten, in: NVwZ – Extra 15/2016, S. 1 (7); vgl. *Matthias Bäcker*, Strategische Telekommunikationsüberwachung auf dem Prüfstand, in: K&R 2014, S. 556 (558 f) zur weiteren Entwicklung einer unscharfen Qualität bis hin zur „Faustregel“.

für die Erhebung von Ausland-Ausland-Verkehren,[258] außer dass G 10-Maßnahmen zum Anlass genommen wurden, eigenständige Routine-Erhebungen durchzuführen.

Huber, Richter am Verwaltungsgericht Frankfurt am Main und langjähriger stellvertretender Vorsitzender der G 10-Kommission, geht deswegen von einer jahrelangen „rechtswidrigen Praxis der Ausland-Ausland-Fernmeldeaufklärung“ aus.[259]

bbb) § 1 Abs. 2 BNDG

Die Bundesregierung vertrat seit dem G 10-Urteil die Ansicht, Abgriffe auf § 1 BNDG stützen zu können.[260] Diese Norm des BNDG schreibt dem Geheimdienst die Aufgabe zu, erforderliche Informationen zu sammeln, um Erkenntnisse über das Ausland von außen- und sicherheitspolitischer Bedeutung zu gewinnen.[261] Inhaltlich ist die Regelung pauschal und weit gefasst. Sie enthält keine Tatbestandsvoraussetzungen, die ein Abgriff konkret zu erfüllen hätte. Der Sachverständige *Bäcker* beschrieb plastisch die möglichen Konsequenzen eines Abgriffs auf dieser Grundlage:

> „Wäre dem zu folgen, so könnte der BND Daten über solche Auslandsverkehre annähernd nach Belieben erheben, auswerten, bevorraten und übermitteln.“[262]

Er folgerte:

---

258) Die Bundesregierung legt den Wortlaut von § 5 Artikel 10-Gesetz („internationale Verkehre“) eng aus und versteht darunter nur die Verkehre mit einem Endpunkt in Deutschland und einem im Ausland; vgl. Darstellung bei *Bäcker*, MAT A SV-2/3, S. 10.

259) *Bertold Huber*, BND-Gesetzreform – gelungen oder nachbesserungswürdig?, in: ZRP 2016, S. 162 (165).

260) Vgl. *A. F.,* Protokoll-Nr. 41 I, S. 155; Auffassung der Bundesregierung, wiedergegeben in BVerfGE 100, 313-403, https://www.bverfg.de/e/rs19990714_1bvr222694.html, Rn. 97; dazu auch *Bäcker*, MAT A SV-2/3, S. 17; *Betrold Huber*, BND-Gesetzreform – gelungen oder nachbesserungswürdig?, in: ZRP 2016, S. 162 (163).

261) Die Debatte findet ihren Anlass im Wortlaut des § 1 „im Geltungsbereich dieses Gesetzes erhoben“, so auch *Graulich*, MAT A SV-11/2, S. 32 ff; kritisch: *Bäcker*, MAT A SV 2/3, S. 17.

262) *Bäcker*, MAT A SV 2/3, S. 1.

> „Grenzen der strategischen Auslandsaufklärung ergeben sich danach praktisch nicht aus dem Recht, sondern fast ausschließlich aus den Ressourcen des BND und dem Ethos seiner Bediensteten.“[263]

ccc) § 2 Abs. 1 BNDG

Der Zeuge *Burbaum*, zu Beginn von EIKONAL G 10-Jurist im BND, befand die allgemeine Befugnisnorm des § 2 BNDG für die Überwachung der „Routine“-Verkehre einschlägig.[264] Sie beinhaltet grundlegende Regelungen über zulässige Zwecke einer Datenerhebung, deren Verhältnismäßigkeit und den Umgang mit Betroffenen. Die Norm verweist immerhin auf datenschutzrechtliche Grenzen und stellt die Datenerhebung u.a. unter den Vorbehalt, dass sie sich auf Vorgänge im Ausland von außen- und sicherheitspolitischer Bedeutung beziehen und ihr Informationsgehalt nicht auf andere Weise zu erlangen ist oder in eine alternative Behördenzuständigkeit fällt. Systematisch enthält sie nur in Abs.1a der damaligen Fassung detaillierte Voraussetzungen, und zwar über das Einholen von Finanzauskünften. Verfahrensrechtliche Vorgaben für geheime Eingriffe in das Fernmeldegeheimnis macht sie jedoch keine. Für einen Abgriff von Telekommunikationsverbindungen bildet sie keine Grundlage.

ddd) Zurechtbiegen des Rechts

> „Solange keine Grundrechtsträger betroffen sind, sind die zum Abschuss freigegeben.“[265]

So formulierte es der Zeuge *T. B.* und weiter:

> „Ich möchte es ein bisschen qualifizieren: Ist in dem Moment freigegeben, in dem ein bestimmtes Ziel dahintersteckt, denn ansonsten wären wir wieder bei der anlasslosen Geschichte (…) Das heißt sie

263) *Matthias Bäcker*, Strategische Telekommunikationsüberwachung auf dem Prüfstand, in: K&R 2014, S. 556 (559f.)

264) *Burbaum* verwies auf § 2 in Zusammenhang mit § 3 BNDG a. F., Protokoll-Nr. 24 I, S. 24 f.

265) *T. B.,* Protokoll-Nr. 20 I, S. 44.

> brauchen eine entsprechende Steuerung, Sie brauchen zusätzliche Informationen, und dann können Sie danach suchen.“[266]

Die Aufstellung von grundrechtsfreien Kategorien im Fernmeldebereich widerspricht verfassungsrechtlicher Wertungen und steht dem BND nicht zu. Solche Rechtsanwendung stellt ein Überstrapazieren der geltenden Rechtslage durch maßlose Auslegung dar, die den Blick auf die Grundrechte verliert und die Geltung des Fernmeldegeheimnisses für Nicht-Deutsche im Ausland in Abrede stellt. Geheimdienst und Bundesregierung haben sich das Recht zurechtgebogen, um ihre Anliegen und Interessen durchzusetzen, anstatt sich einer parlamentarischen Debatte über die Reichweite geheimdienstlicher Praxis zur Ausland-Ausland-Überwachung zu stellen und die verfassungsrechtlichen Grenzen zu berücksichtigen. Der Zeuge *Breitfelder* beschrieb seinen Umgang mit rechtlichen Grenzen:

> „Damit begann auch das Problem, sich an dieses Recht so zu halten, dass auch immer noch ein Nutzen rauskommt – was nicht bedeuten soll, dass wir jetzt am Recht rumgefummelt hätten.“

Die Betonung liegt alleine auf der Aufgabe des Geheimdiensts. Um sie auszufüllen, scheint jedes technisch mögliche Mittel auch opportun. Aus einer Aufgabennorm kann sich aber nie eine Befugnis ableiten lassen, in Grundrechte einzugreifen. Dazu bedarf es vielmehr bereichsspezifischer Gesetze. Da der BND dergleichen nicht hatte, stellte er kurzerhand die Grundrechte für seine Handlungen in Abrede anstatt die Beschränkung der eigenen Befugnisse festzustellen und gegebenenfalls eine Erweiterung durch den Gesetzgeber zu diskutieren. Der BND darf sich auch nicht virtuell ins Ausland flüchten.

eee) Verletzung des Zitiergebots

§§ 1 und 2 BNDG enthielten keinen expliziten Bezug auf das Fernmeldegeheimnis oder auch eine Nennung des Art. 10 GG. Sie verletzten damit das Zitiergebot aus

266) *T. B.,* Protokoll-Nr. 20 I, S. 44.

Art. 10 Abs. 2 GG i. V. m. Art. 19 Abs. 1 Satz 2 GG, nachdem das Fernmeldegeheimnis samt Artikel ausdrücklich in der möglicherweise eingreifenden Norm genannt sein muss.[267] Der Zweck besteht in einer „Warn- und Besinnungsfunktion" gegenüber dem Gesetzgeber, um vor versehentlichen Grundrechtseingriffen zu schützen, und stellt ihn zugleich rechenschaftspflichtig.[268] Der Gesetzgeber muss den Überblick über Überwachungsmaßnahmen behalten, um „kontrollfreie Räume"[269] und eine „globale und pauschale Überwachung"[270] vermeiden zu können. *Huber* schließt daraus, dass die Verantwortlichen bei den Gesetzesnovellen seit 1999 „schlichtweg nicht zur Kenntnis nehmen wollten, dass auch die Speicherung und Nutzung von Telekommunikationsdaten, die der BND im Rahmen der Ausland-Ausland-Überwachung gewonnen hat, den grundrechtlichen Bindungen des Art. 10 GG unterliegt."[271] Anders als in § 8 Abs. 3a BNDG a. F. hat der Gesetzgeber einen grundrechtsbeschränkenden Willen gerade nicht dokumentiert.[272] Es ist insofern davon auszugehen, dass das BNDG das Vorliegen anderer Befugnisnormen voraussetzt, die ihrerseits einen Eingriff in das Fernmeldegeheimnis erlauben, namentlich das Artikel 10-Gesetz. Ferner ist die Auffassung, bei Routine- bzw. Ausland-Ausland-Verbindungen ohne Deutschlandbezug sei Art. 10 GG nicht betroffen, nach dem Vorstehenden nicht haltbar. Verstößt ein Gesetz gegen das Zitiergebot, ist es in dieser Hinsicht formell verfassungswidrig. Somit konnten die §§ 1 und 2 BNDG schon aus formellen Gründen gar keine Grundlage für einen Zugriff auf Daten, die durch das Fernmeldegeheimnis geschützt sind, bilden.[273]

---

267) Vgl. BVerfGE 130, 151–212, https://www.bverfg.de/e/rs20120124_1bvr129905.html, Rn. 173.

268) BVerfGE 64, 72-86, Rn. 29, in: NJW 1983, 2869-2870 Rn. 29; BVerfGE 129, 208–268, https://www.bverfg.de/e/rs20111012_2bvr023608.html, Rn. 178.

269) *Schaar*, Protokoll-Nr. 31 I, S. 28.

270) BVerfG, Urteil vom 14. Juli 1999, 1 BvR 2226,/94, https://www.bverfg.de/e/rs19990714_1bvr222694.html , Rn. 221.

271) *Bertold Huber*, Die strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefugnisse und Regelungsdefizite, in: NJW 2013, S. 2572 (2576)

272) *Papier*, MAT A SV-2/2, S. 7.

273) Vgl. *Johannes Caspar*, Strategische Auslandsüberwachung – Jenseits der Grenze des Rechtsstaats?, in: PinG 2014, H. 1, S. 4; vgl. *Matthias Bäcker*, Strategische Telekommunikationsüberwachung auf dem Prüfstand, in: K&R 2014, S. 556 (560); *Bertold Huber*, Die strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefugnisse und Regelungsdefizite, in: NJW 2013, S. 2572 (2576).

fff) Keine bereichsspezifische und klare Regelung

Wenn Gesetze dazu berechtigen sollen, in das Fernmeldegeheimnis einzugreifen, sind besondere Anforderungen an diese zu stellen. An so einer hinreichenden spezialgesetzlichen Rechtsgrundlage, die den BND hierzu ermächtigt hätte, fehlte es aber. §§ 1 und 2 BNDG verletzen auf materieller Ebene auch das verfassungsrechtliche Bestimmtheitsgebot aus Art. 20 Abs. 3 GG. Eingriffe in das Fernmeldegeheimnis bedürfen einer klaren und bereichsspezifischen Ermächtigungsgrundlage. Am 3. März 2004, also während der Anfänge von EIKONAL, wirkten die damaligen Richter *Papier* und *Hoffmann-Riem* an einem Urteil des BVerfG mit, das die Normenbestimmtheit und -klarheit betreffend Art. 10 GG konkretisierte.[274] Die rechtliche Grundlage muss abstrakt einen Eingriff explizit offenlegen und den Zweck der Verwendung „bereichsspezifisch und präzise“ fassen.[275] Ziel des Bestimmtheitsgebots sind die Erkennbarkeit der Rechtslage, eine Begrenzung des Entscheidungsspielraums in der Verwaltung und die Effektivierung gerichtlicher Kontrolle.[276] Konkrete Anforderungen richten sich nach der Intensität der Eingriffe. Bei geheimen Maßnahmen mit großer Streubreite kommt gesetzlichen Vorgaben ein besonderes Gewicht zu.[277]

274) BVerfGE 110, 33 – 76, https://www.bverfg.de/e/fs20040303_1bvf000392.html, Rn. 103ff; diesen Einwand gegen § 1 BNDG brachten die Beschwerdeführer_innen im G 10-Verfahren schon 1999 vor, damals wurde allerdings nicht diesbezüglich entschieden, vgl. Beschwerdeführer_innen in BVerfGE 100, 313-403, https://www.bverfg.de/e/rs19990714_1bvr222694.html, Rn. 70.

275) BVerfGE 100, 313-403, https://www.bverfg.de/e/rs19990714_1bvr222694.html, Rn. 165 und 259; vgl. BVerfGE 110, 33 – 76, https://www.bverfg.de/e/fs20040303_1bvf000392.html, Rn. 107; BVerfGE 125, 260-385, http://www.bverfg.de/e/rs20100302_1bvr025608.html, Rn.226; vgl. *Hans-Jürgen Papier*, Beschränkungen der Telekommunikationsfreiheit durch den BND an Datenaustauschpunkten, in: NVwZ – Extra 15/2016, S. 1 (8).

276) Vgl. BVerfGE 100, 313-403, https://www.bverfg.de/e/rs19990714_1bvr222694.html, Rn. 280; BVerfGE 110, 33 – 76, https://www.bverfg.de/e/fs20040303_1bvf000392.html, Rn. 109f: „Je ungenauer die Ziele einer Normierung und die Anforderungen an die tatsächliche Ausgangslage gesetzlich umschrieben sind, umso schwerer fällt die Beurteilung der Eignung und Erforderlichkeit einer Überwachungsmaßnahme.“

277) Vgl. BVerfGE 100, 313-403, https://www.bverfg.de/e/rs19990714_1bvr222694.html, Rn. 270.

Für Maßnahmen der strategischen Fernmeldeüberwachung muss die gesetzliche Klarstellung besondere Regelungen für zeitliche, sachliche und geografische Begrenzung der Überwachungskapazität[278] sowie die Erstellung und Verwendung von Selektoren[279] und einen Verzicht auf Identifizierungsmerkmale in den Suchkriterien[280] umfassen. Soweit Inhaltsdaten erfasst werden oder Metadaten zur Erstellung von individualisierten Persönlichkeitsprofilen verwendet werden, sind konzeptionell schon im Gesetz Maßnahmen zum Schutze des unantastbaren Kernbereichs privater Lebensführung vorzusehen. Außerdem sind Datensicherheitsstandards und Benachrichtigungspflichten festzulegen.[281] Überwachungsanlass und -gegenstand, Zweck, Verfahren der Erhebung, Weiterverarbeitung, Bevorratung und Übermittlung sowie Löschungspflichten, Kennzeichnugspflichten, Kontrollmechanismen und unabhängige Überprüfungen als Kompensation fehlenden Rechtsschutzes für die Betroffenen müssen klar geregelt sein.[282] Sie stellen organisatorische und verfahrensrechtliche Absicherungen dar. Der Sachverständige *Bäcker* erhob unter diesen Voraussetzungen

278) Vgl. *Hans-Jürgen Papier*, Beschränkungen der Telekommunikationsfreiheit durch den BND an Datenaustauschpunkten, in: NVwZ – Extra 15/2016, S. 1 (10)*; Bertold Huber*, BND-Gesetzreform – gelungen oder nachbesserungswürdig?, in: ZRP 2016, S. 162 (163); *Johannes Caspar*, Strategische Auslandsüberwachung – Jenseits der Grenze des Rechtsstaats?, in: PinG 2014, H. 1, S. 1 (5).

279) Vgl. kritische Ausführungen zu Selektoren und ihrer Weiterentwicklung über einfache Suchbegriffe hinaus bei *Frank Braun*, Die strategische Fernmeldekontrolle durch den Bundesnachrichtendienst, in AnwaltszertifikatOnline IT- und Medienrecht 8/2015, Rn. 3, zur Suche mit Ähnlichkeitsfunktion, vgl. BVerfGE 130, 151 – 212, https://www.bverfg.de/e/rs20120124_1bvr129905.html, Rn. 73 Beschwerdeführer; gegen Notwendigkeit einer zeitlichen und sachlichen Kapazitätsbeschränkung*: Wilfried Karl/Michael Soiné*, Neue Rechtsgrundlagen für die Ausland-Ausland-Fernmeldeaufklärung, in: NJW 2017, S. 919 (920).

280) Vgl. § 5 Artikel 10-Gesetz in der Fassung vom 26. Januar 2001; *Johannes Caspar* , Strategische Auslandsüberwachung – Jenseits der Grenze des Rechtsstaats?, in: PinG 2014, H. 1, S. 1 (5).

281) Vgl. BVerfGE 125, 260-385, http://www.bverfg.de/e/rs20100302_1bvr025608.html, Ls.2; BVerfGE 129, 208–268, https://www.bverfg.de/e/rs20111012_2bvr023608.html, Rn. 231; BVerfGE 130, 151–212, https://www.bverfg.de/e/rs20120124_1bvr129905.html, Rn. 186.

282) Ausführungen zu den einzelnen Anforderungen, vgl. BVerfGE 100, 313-403, https://www.bverfg.de/e/rs19990714_1bvr222694.html, Rn. 304; *Bäcker*, MAT A SV 2/3, S. 17; *Hans-Jürgen Papier*, Beschränkungen der Telekommunikationsfreiheit durch den BND an Datenaustauschpunkten, in: NVwZ – Extra 15/2016, S. 1 (7); *Johannes Caspar*, Strategische Auslandsüberwachung – Jenseits der Grenze des Rechtsstaats?, in: PinG 2014, H. 1, S. 1 (4 f.); siehe auch Ausführungen zur erhöhten Gefahr eines Ringtausches bei fehlenden Übermittlungsvorschriften bei *Frank Braun*, Die strategische Fernmeldekontrolle durch den Bundesnachrichtendienst, in AnwaltszertifikatOnline IT- und Medienrecht 8/2015, Rn. 3.

schwerwiegende Bedenken im Hinblick auf die Bestimmtheit der herangezogenen Normen.

> „Die Rechtsauffassung der Bundesregierung verkennt jedoch den räumlichen Anwendungsbereich und den extraterritorialen Schutzgehalt des Fernmeldegeheimnisses des Art. 10 GG. Von Verfassungswegen bedarf auch die Auslandsaufklärung des BND einer formellgesetzlichen Ermächtigung, die den Geboten der Bestimmtheit und Verhältnismäßigkeit genügt.“[283]

Er stellte als Ergebnis seiner Untersuchungen fest:

> „All dies leistet § 1 Abs. 2 Satz 1 BNDG für sich genommen evident nicht.“[284]

Ein Abgriff auf der Grundlage von § 1 Abs. 2 BNDG ist verfassungswidrig. Der erste Paragraph des BND-Gesetzes ist eine einleitende Aufgabenbeschreibung und enthält keine eigenständige Ermächtigung.[285] *Hoffmann-Riem* hob hervor, dass es keine nachrichtendienstliche Datenerfassung außerhalb des Geltungsbereichs der Rechtsordnung geben kann:

> „§ 1 Abs. 2 S. 1 BNDG erlaubt nicht den Schluss, dass eine Erhebung oder Auswertung durch den BND mit Hilfe von Einrichtungen, die nicht im deutschen Hoheitsgebiet gelegen sind, keinen rechtlichen Restriktionen nach deutschem Recht unterliegen. Dies wäre mit Art. 10 GG nicht vereinbar.“[286]

---

283) *Bäcker,* MAT A SV-2/3, S. 1.

284) *Bäcker*, MAT A SV-2/3, S. 18.

285) Vgl. BVerfG-Rechtsprechung zu § 39 AWG als pauschale Aufgabenbeschreibung in BVerfGE 110, 33 – 76, https://www.bverfg.de/e/fs20040303_1bvf000392.html, Rn. 118; zum Generalklauselbegriff, BVerfGE 125, 260-385, http://www.bverfg.de/e/rs20100302_1bvr025608.html, Rn. 228; zu § 1 BNDG *Hoffmann-Riem*, MAT A SV-2/1-neu, S. 11; *Berthold Huber*, Die strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefugnisse und Regelungsdefizite, in: NJW 2013, S. 2572 (2576); *Hans-Jürgen Papier*, Beschränkungen der Telekommunikationsfreiheit durch den BND an Datenaustauschpunkten, in: NVwZ – Extra 15/2016, S. 1 (7).

286) *Hoffmann-Riem*, MAT A SV-2/1-neu, S. 11, mit weiteren Verweisen.

Auch § 2 BNDG ist als allgemeine Befugnisnorm angesichts der Eingriffsintensität zu pauschal gefasst, als dass sie selbstständig eine strategische Auslandsaufklärung rechtfertigen könnte.[287] Die Norm wird den Anforderungen, die an Beschränkungen des Fernmeldegeheimnisses zu stellen sind nicht gerecht. Johannes Caspar, Landesdatenschutzbeauftragter in Hamburg, fasst das treffend wie folgt zusammen:

> „Allein der allgemeine Hinweis auf Vorgänge im Ausland, die von außen- und sicherheitspolitischer Bedeutung für die Bundesrepublik Deutschland sind, kann eine umfassende massenhafte Speicherung und Auswertung von Kommunikationsverbindungen ins Blaue hinein nicht rechtfertigen."[288]

Es bleibt festzustellen, dass auch die eingangs zitierte, für den BND insgesamt repräsentative Auffassung, wonach Überwachungsmaßnahmen, wenn sie nur im Ausland stattfinden, keine „Genehmigung" bedürfen, jeder verfassungsrechtlichen Grundlage entbehren.

c) Datenausleitung durch [redacted]

[redacted]

[redacted]

---

287) Vgl. *Hans-Jürgen Papier*, Beschränkungen der Telekommunikationsfreiheit durch den BND an Datenaustauschpunkten, in: NVwZ – Extra 15/2016, S. 1 (7); Frank Braun, Die strategische Fernmeldekontrolle durch den Bundesnachrichtendienst, in AnwaltszertifikatOnline IT- und Medienrecht 8/2015, Rn. 3; *Berthold Huber*, Die strategische Rasterfahndung des Bundesnachrichtendienstes – Eingriffsbefugnisse und Regelungsdefizite, in: NJW 2013, S. 2572 (2576); auch § 3 BNDG in der Fassung vom 20. Dezember 1990 genügt diesen Anforderungen nicht (vgl. *Huber* & *Papier* ebenda).

288) *Johannes Caspar*, Strategische Auslandsüberwachung – Jenseits der Grenze des Rechtsstaats?, in: PinG 2014, H. 1, S. 1 (4 f.).

[redacted]

[redacted]

> [redacted]

[redacted]

289) *Uhrlau*, 1. Untersuchungsausschuss der 16. Wahlperiode, Protokoll-Nr. 119, S. 135.

290) *Uhrlau*, 1. Untersuchungsausschuss der 16. Wahlperiode, Protokoll-Nr. 119, S. 136.

aa) Rechtsgrundlagen von TK-Anbietern für Datenausleitung an BND

aaa) Grundrechtsbindung Privater bei der Ausführung hoheitlicher Aufgaben

Art. 1 Abs. 3 GG bindet alle staatliche Gewalt, sei es Gesetzgebung, Exekutive oder Rechtsprechung, an die Grundrechte als unmittelbar geltendes Recht. Staatliche Maßnahmen, insbesondere der „vollziehenden Gewalt“, müssen sich also an den Grundrechten ausrichten und bedürfen einer ihrerseits verhältnismäßigen gesetzlichen Grundlage, sobald sie grundrechtlich garantierte Freiheiten tangieren. Dabei spielt es zunächst keine Rolle, ob sich der Staat zur Erfüllung seiner Aufgaben der von ihm auf verschiedenen Stufen eingerichteten Verwaltungsbehörden bedient, die durch hoheitliche Anordnungen oder durch Vollziehung mit eigenen Mitteln agieren, oder die Erledigung seiner Aufgaben privatrechtlich organisierten Unternehmen überlässt, die auf zivilgesetzliche Handlungsformen ohne hoheitliche Befugnisse verpflichtet sind und vom Staat lediglich kontrolliert werden. Denn es soll dem Staat verwehrt sein, sich durch „eine Flucht in das Privatrecht“ seiner Grundrechtsbindung zu entziehen.[291] Bis zu einer klärenden Entscheidung des Bundesverfassungsgerichts (BVerfG) im Jahre 2011[292] war jedoch umstritten, ob und inwieweit die Beteiligung des Staates an Privatunternehmen (sog. gemischt-wirtschaftliche Unternehmen) diese zu Grundrechtsverpflichteten macht.

[redacted]

291) Vgl. *Klaus Lederer*, Flucht ins Privatrecht, Technokratisierung, Ökonomisierung und Entdemokratisierung als Herausforderung für die progressive Rechtswissenschaft, in: Plöse/Fritsche/Kuhn/Lüders, Festschrift für Rosemarie Will, Berlin 2016, S. 429 ff.

292) BVerfGE 128, 226 (244ff.), https://www.bverfg.de/e/rs20110222_1bvr069906.html.

[redacted]

[redacted]

293) In der dafür notwendigen Anpassung des Grundgesetzes wurden die Bestimmungen des Art. 87 GG, nach denen die Deutsche Bundespost in bundeseigener Verwaltung mit eigenem Verwaltungsunterbau geführt werden musste, geändert und mit dem neu geschaffenen Art. 87 f GG ein Privatisierungsauftrag sowie in dessen Abs. 2 eine Verpflichtung zur Liberalisierung des TK-Marktes geschaffen.

294) Mit 14,34% unmittelbar und mit 17,45% mittelbar über die staatseigene Kreditanstalt für Wiederaufbau (KfW), vgl. Bundesministerium der Finanzen, Die Beteiligungen des Bundes, Beteiligungsbericht 2016, S. 13, 35 f.

295) *Deutsche Telekom AG*, Geschäftsbericht 2003, S. 39.

296) Vgl. *Peter M. Huber*, Öffentliches Wirtschaftsrecht, in: Eberhard Schmidt-Aßmann/ Friedrich Schoch (Hrsg.), Besonderes Verwaltungsrecht, 14. Auflage, Berlin 2008, S. 448 f.

297) *Alster*, Protokoll-Nr. 30 II – Auszug offen, S. 24.

298) BGHZ 36, 91, 95 f.; 91, 84, 96 f. Im Übrigen sollten die privatwirtschaftlich agierenden staatlichen Organe wie Privatrechtssubjekte behandelt werden.

[redacted]

[redacted]

---

299) BVerfG NJW 1990, 1783; ähnlich VerfGH Berlin, DÖV 2005, 515 ff. (unabhängig davon, ob die Wahrnehmung öffentlicher Aufgaben betroffen ist).

300) Vgl. *Dirk Ehlers*, Verwaltung und Verwaltungsrecht im demokratischen und sozialen Rechtsstaat, in: Hans-Uwe Erichsen/ Dirk Ehlers, Allgemeines Verwaltungsrecht, 13. Auflage, Berlin 2005, S. 157.

301) BVerwGE 114, 160 (189); 118, 226 (238); BVerwG NVwZ 2004, 745.

302) Vgl. *Dirk Ehlers*, Verwaltung und Verwaltungsrecht im demokratischen und sozialen Rechtsstaat, in: Hans-Uwe Erichsen/ Dirk Ehlers, Allgemeines Verwaltungsrecht, 13. Auflage, Berlin 2005, S. 157

303) Vgl. *Klaus Lederer* Flucht ins Privatrecht, Technokratisierung, Ökonomisierung und Entdemokratisierung als Herausforderung für die progressive Rechtswissenschaft, in: Plöse/Fritsche/Kuhn/Lüders, Festschrift für Rosemarie Will, Berlin 2016, S. 429 (432 f.)

[redacted]

[redacted]

[redacted]

304) BVerfGE 128, 226 (246 f.), https://www.bverfg.de/e/rs20110222_1bvr069906.html; dazu *Jan Philipp Schaefer*, Neues vom Strukturwandel der Öffentlichkeit, Gewährleistungsverwaltung nach dem Fraport-Urteil des Bundesverfassungsgerichts, Der Staat Vol. 51 (2012), No. 2, S. 251–277 (259 f.).

305) BVerfGE 128, 226 (249), https://www.bverfg.de/e/rs20110222_1bvr069906.html.

306) BVerfGE 128, 226 (249 f.), https://www.bverfg.de/e/rs20110222_1bvr069906.html.

307) Zur schon damals anerkannten unmittelbaren Grundrechtsbindung von Beliehenen vgl. *Hans Dieter Jarass*, in: Jarass/Pieroth, Grundgesetz für die Bundesrepublik Deutschland, Kommentar, 6. Auflage, München 2002, Art. 1 Rn. 30 m.w.N.

bbb) Fernmeldegeheimnis, § 88 Telekommunikationsgesetz (TKG)[308]

Als Telekommunikationsunternehmen trägt [redacted] eine besondere rechtliche Verantwortung und ist dem Schutz des Fernmeldegeheimnisses nach § 88 TKG verpflichtet.[309] Die unbefugte Datenweitergabe ist zudem nach StGB, TKG sowie BDSG eine rechtswidrige Tat und strafbewehrt.[310] Es bestehen explizite Verbote gegen die unbefugte Verschaffung, Kenntnisnahme und Weitergabe. Gem. § 4 Abs. 1 BDSG stehen die Erhebung, Verarbeitung und Nutzung personenbezogener Daten unter einem Erlaubnisvorbehalt.[311] Jegliche Datenverwendung muss daher aufgrund einer gesetzlichen Befugnis erlaubt sein oder auf die Einwilligung des Betroffenen gestützt werden können. Wegen der Heimlichkeit der Ausleitung von Datenströmen durch den TK-Anbieter scheidet eine Einwilligung der Nutzer_innen dieser Infrastrukturangebote regelmäßig aus. Es bedarf einer spezialgesetzlichen Ermächtigung. Für die Weitergabe von Kenntnissen aus Kommunikationsvorgängen stellt darüber hinaus § 88 Abs. 3 TKG als Spezialgesetz die zusätzliche Hürde einer gesonderten gesetzlichen Regelung auf. Nach dieser gesetzlichen Übermittlungsvoraussetzung wäre daher auch eine (mutmaßliche) Einwilligung der Betroffenen nicht ausreichend. Vielmehr bedarf es nach § 88 Abs. 3 Satz 3 TKG (damals § 85 Abs. 3 Satz 3 TKG a. F.) im verfassungsrechtlich durch Art. 10 GG verbürgten Schutzbereich des Fernmeldegeheimnisses in jedem Einzelfall einer spezialgesetzlichen Ermächtigung[312] für „eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere“ (zur Reichweite des Schutzbereichs von Art. 10 siehe oben V.3.b)bb)). Eine solche Ver-

308) Das TKG wurde am 22. Juni 2004 neu gefasst; die Regelungen des § 88 waren bis zu diesem Zeitpunkt in § 85 TKG a. F. angelegt.

309) § 88 Abs. 2 Satz 1 TKG: „Zur Wahrung des Fernmeldegeheimnisses ist jeder Diensteanbieter verpflichtet.“ (vor 22. Juni 2004: § 85 TKG a. F.).

310) Vgl. §§ 201–206 StGB (teils in den Fassungen von 13. November 1998 u.a.), § 148 TKG (in der Fassung vom 26. Juni 2006), § 43 BDSG (in der Fassung vom 14. Januar 2003); BGH 2 StR 591/11, Rn. 21.

311) Vgl. *Bettina Sokol,* in: Simitis (Hrsg.), Bundesdatenschutzgesetz, 7. Auflage, Baden-Baden 2011, § 4 Rn. 4 ff.; so auch BGH 2 StR 591/11, Rn. 23 in: NJW 2013, S. 401-404.

312) § 88 Abs. 3 Satz 3 TKG (§ 85 Abs. 3 Satz 3 TKG a. F.) setzt insofern für eine zweckfremde Verwendung der Daten bzw. eine Weitergabe voraus, dass entweder das TKG selbst oder „eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht.“

pflichtung der TK-Anbieter zur Erteilung von Auskünften gegenüber den Sicherheitsbehörden ist für Verbindungs- und Verkehrsdaten in § 113 TKG sowie für das Abschöpfen von Inhaltsdaten in § 2 Artikel 10-Gesetz geregelt. Beide Ermächtigungsbestimmungen für die TK-Dienstleister setzen jedoch ihrerseits entsprechende Erhebungsbefugnisse der Sicherheitsbehörden voraus.

Das gesetzlich vorgesehene Verfahren für Abhörmaßnahmen nach den §§ 5 ff. Artikel 10-Gesetz wurde jedoch gerade nicht angewendet.

ccc) Formalisiertes Anordnungsverfahren: das G 10-Regime

Ob eine G 10-Anordnung den Abgriff von Transitdaten in diesem Umfang überhaupt hätte rechtfertigen könne, ist an dieser Stelle nicht zu klären (vgl. dazu die Ausführungen unten V.4 – EIKONAL – G 10-Anordnung als „Türöffner“). Nachfolgend soll lediglich das „übliche Verfahren“ kurz dargestellt werden.

Jenseits von Individualmaßnahmen, die nur aufgrund tatsächlicher Anhaltspunkte für eine Verdacht terroristischer Vorbereitungshandlungen, des Landes-, Hoch- oder Friedensverrats, der gewerblichen Schleusungskriminalität oder nunmehr auch einer Straftat nach dem Völkerstrafgesetzbuch nach § 3 Artikel 10-Gesetz oder nach § 100a der StPO bzw. einschlägiger Regelungen in den Landespolizeigesetzen gegen konkrete Personen ergehen dürfen, dient die strategische Fernmeldeaufklärung des BND erst der Gewinnung von Verdachtsmomenten in Bezug auf Proliferation von Gütern, die unter das Kriegswaffenkontrollgesetz fallen, Terrorismus, schwere Geldwäsche und Migrationsdelikte. Hier werden bestimmte Telekommunikationsverkehre von Deutschland ins Ausland oder umgekehrt wie bei einer Rasterfahndung nach bestimmten Suchbegriffen (Selektoren) gefiltert. Diese strategische Fernmeldeaufklärung richtet sich nach § 5 Artikel 10-Gesetz.

Dazu müssen zunächst die Staaten, gegen die sich die Auslandsaufklärung des BND richten darf, vom Parlamentarischen Kontrollgremium des Bundestages (PKGr) festgelegt werden. Auf dieser Grundlage kann seitens des BND durch dessen Präsidenten oder Stellvertreter über das Bundesministerium des Innern ein Antrag nach § 5 Artikel 10-Gesetz bei der vom PKGr eingesetzten G 10-Kommission gestellt werden, die

einer entsprechenden Überwachungsmaßnahme vorab zustimmen muss. Der ausführlich zu begründende Antrag enthält eine Liste mit Suchbegriffen von Inhalts- und Metadaten und ist zeitlich zu befristen. Die Anordnung darf sich stets nur auf die Telekommunikation zwischen Deutschland und dem Ausland bzw. dem Ausland und Anschlüssen in Deutschland, aber weder im Ausland noch im Inland gezielt auf konkrete Anschlüsse beziehen, sofern deutsche Staatangehörige davon betroffen werden können (§ 5 Abs. 2 Artikel 10-Gesetz, sonst nämlich nur nach § 3 Artikel 10-Gesetz).[313] Dabei ist nach § 10 Abs. 4 Satz 3 Artikel 10-Gesetz sicherzustellen, dass der Anteil der überwachten Kommunikation 20 Prozent der auf den Übertragungswegen zur Verfügung stehenden Leitungskapazität nicht überschreitet, was wegen der geringen Auslastung auch oft nicht nötig ist, um den gesamten Verkehr zu erfassen.[314] Darüber hinaus bestehen Möglichkeiten zur strategischen Überwachung nur nach § 8 Artikel 10-Gesetz bei Gefahr für Leib oder Leben einer Person, was in der Regel bei Entführungsfällen vorkommt.

[redacted]

> [redacted]“[315]

---

313) Vgl. *Bertold Huber*, Die strategische Rasterfahndung des Bundesnachrichtendienstes, Eingriffsbefugnisse und Regelungsdefizite, NJW 2013, S. 2572 ff.; ders., Die Fernmeldeaufklärung des Bundesnachrichtendienstes, Rechtsgrundlagen und bestehende Regelungsdefizite, vorgänge #206/207 (2014), S. 42 ff.

314) Vgl. *Bäcker*, MAT A SV-2/3, S. 11 f.

315) *Helfrich*, Protokoll-Nr. 30 I, S. 40.

[redacted]

> [redacted]

[redacted]

bb) Abwegige Rechtskonstruktionen für EIKONAL

aaa) Die Verwaltungshelferthese

[redacted]

316) *Alster*, Protokoll-Nr. 30 I, S. 71.

317) *Alster*, Protokoll-Nr. 30 I, S. 77.

318) *Alster*, Protokoll-Nr. 30 I, S. 69.

[redacted]

(1) TK-Betreiber ist kein Abschleppunternehmen

[redacted]

---

319) § 15 Abs. 2 BDSG, der nur nachrangig zu den Spezialvorschriften des Artikel 10-Gesetz gilt, lautet: „Die Verantwortung für die Zulässigkeit der Übermittlung trägt die übermittelnde Stelle. Erfolgt die Übermittlung auf Ersuchen des Dritten, an den die Daten übermittelt werden, trägt dieser die Verantwortung. In diesem Fall prüft die übermittelnde Stelle nur, ob das Übermittlungsersuchen im Rahmen der Aufgaben des Dritten, an den die Daten übermittelt werden, liegt, es sei denn, dass besonderer Anlass zur Prüfung der Zulässigkeit der Übermittlung besteht."

320) [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

321) *Dr. Köbele*, Protokoll-Nr. 33 I, S. 134 f.

322) *Dr. Köbele*, Protokoll-Nr. 33 I, S. 137.

323) *Dr. Köbele*, Protokoll-Nr. 33 I, S. 137.

324) *Dr. Köbele*, Protokoll-Nr. 33 I, S. 145 f.

325) *Hartmut Maurer*, Allgemeines Verwaltungsrecht, 18. Auflage 2011, § 23 Rn. 59.

326) Vgl. *Rolf-Rüdiger Schenke*, Polizei- und Ordnungsrecht, 6. Auflage 2009, Rn. 710 ff.

[redacted]

(2) Rechtliche Verantwortung [redacted]

[redacted]

327) BGH, Urteil vom 14. Oktober 2004, Az. III ZR 169/04, BGHZ 161, 6-14, Rn. 18.

328) Vgl. *Fritz Ossenbühl*, Staatshaftungsrecht, 5. Auflage 1998, S. 13 ff.

329) *Hartmut Maurer*, Allgemeines Verwaltungsrecht, 18. Auflage 2011, § 23 Rn. 59; *Ulmer*, CR 2003, S.703 f.

330) BVerfGE 125, 260 (348), http://www.bverfg.de/e/rs20100302_1bvr025608.html.

[redacted]

[redacted]

331) Vgl. §§ 110–114 TKG (in der Fassung vom 22. Juni 2004 sowie der Fassung vom 31. Oktober 2006), § 2 Artikel 10-Gesetz (in der Fassung vom 22. Juni 2004) und § 5 Artikel 10-Gesetz (in der Fassung vom 26. Juni 2001, § 8 Abs. 8 BVerfSchG (in der Fassung vom 9. Januar 2002; seit dem Gesetz zur Ergänzung des Terrorismusbekämpfungsgesetzes vom 5. Januar 2007 in § 8a Abs. 2 Satz 1 Nr. 4 BVerfSchG geregelt) sowie in § 2a BNDG (seit dem Gesetz vom 23. Dezember 2016 nunmehr in § 3 BNDG) und in § 4 MADG.

[redacted]

[redacted]

[redacted]

332) BVerfGE 100, 313 (376, 391 f.), https://www.bverfg.de/e/rs19990714_1bvr222694.html.

333) BVerfGE 67, 157 (174), http://www.servat.unibe.ch/dfr/bv067157.html .

334) BVerfGE 100, 313 (376 f., 384), https://www.bverfg.de/e/rs19990714_1bvr222694.html.

335) Fassung vom 9. Januar 2002. Vgl. dazu die im Urteil des BVerfG vom 14. Juni 1999, BVerfGE 100, 313 (339 f.), https://www.bverfg.de/e/rs19990714_1bvr222694.html, wiedergegebene Stellungnahme des Bundesministers des Inneren, der sich insoweit auf einen Bericht des Präsidenten des BND bezieht. Später auch noch in Bundestagsdrucksache 17/9640 vom 15. Mai 2012 (S. 6) und 17/14739 vom 12. September 2013 (S. 9).

336) BVerfGE 100, 313 (376), https://www.bverfg.de/e/rs19990714_1bvr222694.html.

[redacted]

> [redacted]

[redacted]

(3) Keine Datenverarbeitung im Auftrag (§ 11 BDSG)

[redacted]

---

337) Vgl. BVerfGE 130, 151 – 212, https://www.bverfg.de/e/rs20120124_1bvr129905.html, Rn. 12.

[redacted]

(4) Zwischenergebnis

[redacted]

bbb) Der Freibrief des Kanzleramtes

Der sogenannte *Freibrief* des Bundeskanzleramts erschöpft sich in einer kurzen Bestätigung der Rechtsauffassung des BND, ohne diese argumentativ zu begründen. [redacted]

(1) Eindruck auf [redacted]

[redacted]

---

338) *Thilo Weichert*, in: Däubler/ Klebe/ Wedde/ Weichert, Bundesdatenschutzgesetz. Kompaktkommentar zum BDSG, 4. Aufl. 2014, § 11 Rn. 18.

339) *Thilo Weichert*, in: Däubler/ Klebe/ Wedde/ Weichert, Bundesdatenschutzgesetz. Kompaktkommentar zum BDSG, 4. Aufl. 2014, § 3 Rn. 54.

340) *Thomas Petri*, in: Simitis (Hrsg.), Bundesdatenschutzgesetz, Kommentar, 7. Auflage 2011, § 11 Rn. 12.

[redacted]

> [redacted]

[redacted]

> [redacted]

> [redacted]

[redacted][346]

---

341) *S. L.,* Protokoll-Nr. 26 I, S. 24.

342) *Dr. Köbele*, Protokoll-Nr. 33 I, S. 134 f.

343) *S. L.*, Protokoll-Nr. 26 I, S. 24.

344) *S. L.*, Protokoll-Nr. 26 I, S. 24.

345) *S. L.,* Protokoll-Nr. 26 I, S. 24.

346) *Ricke*, Protokoll-Nr. 26 I, S. 113.

[redacted]

(2) Rechtliche Bewertung

[redacted]

[redacted]

347) [redacted]

348) [redacted]

349) [redacted]

[redacted]

[redacted]

[redacted]

ccc) Geschäftsbesorgungsvertrag über Transitdaten

[redacted]

> [redacted]

[redacted]

[redacted]

[redacted]

350) [redacted]

351) *S. L.*, Protokoll-Nr. 26 I, S. 24 f.

352) *Alster*, Protokoll-Nr. 30 II – Auszug offen, S. 24.

353) *Dr. Köbele*, Protokoll-Nr. 33 I, S. 148.

354) § 88 Abs. 3 TKG; vgl. Artikel 10-Gesetz i. V. m. TKÜV (bis 22. Juni 2004: § 85 TKG a. F.).

[redacted]

[redacted]

[redacted][358]

ddd) Zwischenergebnis: Ausleitung erfolgt ohne Rechtsgrundlage

[redacted]

355) [redacted]

356) [redacted]

357) [redacted]

358) [redacted]

[redacted]

cc) Rechtswidrige Handlungen [redacted]

aaa) Schaltauftrag [redacted]

[redacted]

[redacted]

> [redacted]

[redacted]

> [redacted]

---

359) *Alster*, Protokoll-Nr. 30 II – Auszug offen, S. 22.

360) *Helfrich*, Protokoll-Nr. 30 I, S. 37.

361) *Alster*, Protokoll-Nr. 30 I, S. *88*.

362) *Alster*, Protokoll-Nr. 30 I, S. 70.

[redacted]

bbb) Doppelung und Datenweitergabe

[redacted]

> [redacted]

---

363) *Helfrich*, Protokoll-Nr. 30 I, S. 26, 37, 43.

364) *Alster*, Protokoll-Nr. 30 I, S. 73.

365) *Alster*, Protokoll-Nr. 30 I, S. 73.

366) *Helfrich*, Protokoll-Nr. 30 I, S. 16 f.

367) *Alster*, Protokoll-Nr. 30 II – Auszug offen, S. 7.

[redacted]

> [redacted]

> [redacted]

[redacted]

> [redacted]

> [redacted]

368) *S. L.,* Protokoll-Nr. 26 I, S. 8.

369) *Helfrich*, Protokoll-Nr. 30 I, S. 16.

370) *S. L.,* Protokoll-Nr. 26 I, S. 8.

371) *S. L.*, Protokoll-Nr. 26 I, S. 40.

372) *Dr. Burbaum*, Protokoll-Nr. 24 I, S. 24.

373) *Alster*, Protokoll-Nr. 30 II – Auszug offen, S. 6.

[redacted]

ccc) Rechtliche Bedenken [redacted]

[redacted]

374) *Ullrich Dammann*, in: *Simitis* (Hrsg.), Bundesdatenschutzgesetz, Kommentar, 7. Auflage, § 1, Rn. 238: „Werden solche Daten jedoch für andere Zwecke verwendet, weitergehend aufbewahrt oder zur Kenntnis genommen, so entfällt die Privilegierung. Auf die Auftragsdatenverarbeitung ist die Transitregelung nicht, auch nicht entsprechend, anzuwenden.“

375) [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

376) *Dr. Köbele*, Protokoll-Nr. 33 I, S. 142.

377) *Dr. Köbele*, Protokoll-Nr. 33 I, S. 128.

378) *Dr. Köbele*, Protokoll-Nr. 33 I, S. 142.

379) *Alster*, Protokoll-Nr. 30 I, S. 94: [redacted] vgl. *Helfrich*, Protokoll-Nr. 30 I, S. 31.

380) *Alster*, Protokoll-Nr. 30 I, S. 77.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

dd) Strafrechtliche und zivilrechtliche Beurteilung

[redacted]

381) *Alster*, Protokoll-Nr. 30 II – Auszug offen, S. 15.

382) *Alster*, Protokoll-Nr. 30 I, S. 68.

383) *Alster*, Protokoll-Nr. 30 II – Auszug offen, S. 28.

384) Vgl. *Alster*, Protokoll-Nr. 30 II – Auszug offen, S. 54.

385) *Dr. Köbele*, Protokoll-Nr. 33 II – Auszug offen, S. 19 f.

[redacted]

aaa) Strafrechtliche Konsequenzen

[redacted]

[redacted]

> [redacted]

386) Vgl. §§ 201 – 206 StGB (teils in den Fassungen vom 13. November 1998) , § 43 BDSG (in der Fassung vom 14. Januar 2003); BGH, Urteil vom 10. Oktober 2012, 2 StR 591/11, Rn. 21 in: NJW 2013, S. 401-404.

387) Vgl. *Kai Cornelius*, Strafrechtliche Verantwortlichkeiten bei der Strategischen Telekommunikationsüberwachung, JuristenZeitung 14/2015, S. 693 (695 f.).

388) Vgl. BGH, Urteil vom 10. Oktober 2012, 2 StR 591/11, Rn. 22 f. in NJW 2013, S. 401-404

389) *S. L.,* Protokoll-Nr. 26 II – Auszug offen, S. 6.

[redacted]

[redacted]

> [redacted]

[redacted]

390) *Kai Cornelius*, Strafrechtliche Verantwortlichkeiten bei der Strategischen Telekommunikationsüberwachung, JuristenZeitung 14/2015, S. 693 (700 f.) m. w. N.

391) *Theodor Lenckner*, in: Festschrift für *Stree/Wessels*, 1993, S. 235.

392) *Andreas Hoyer*, Strafrechtliche Verantwortlichkeit innerhalb von Weisungsverhältnissen, 1998, S. 13.

393) *Kai Cornelius*, Strafrechtliche Verantwortlichkeiten bei der Strategischen Telekommunikationsüberwachung, JuristenZeitung 14/2015, S. 693 (701).

[redacted]

> [redacted]

[redacted]

[redacted]

394) *Papier*, MAT A SV 2/2, S. 9

395) BVerfGE 125, 260-385, http://www.bverfg.de/e/rs20100302_1bvr025608.html, Rn. 252 m.w.N.

396) [redacted]

397) BGH, Urteil vom 10. Oktober 2012, Az. 2 StR 591/11 in NJW 2013, S. 401-404.

398) [redacted]

[redacted]

bbb) Zivilrechtliche Haftung

[redacted]

399) [redacted]

400) Vgl. *Hans-Jürgen Papier*, Beschränkungen der Telekommunikationsfreiheit durch den BND an Datenaustauschpunkten, NVwZ – Extra 15/2016, S. 1 (4), abrufbar unter http://rsw.beck.de/rsw/upload/NVwZ/NVwZ-Extra_2016_15.pdf: „Von strategischen Beschränkungen können überhaupt nur die in Anspruch genommenen Telekommunikationsdienstleister erfahren, für die eigentlichen Teilnehmer des Telekommunikationsverkehrs bleiben sie in aller Regel unbekannt.“

401) Vgl. *Springer Gabler Verlag* (Herausgeber), Gabler Wirtschaftslexikon, Stichwort: Carrier, abrufbar unter: http://wirtschaftslexikon.gabler.de/Archiv/75651/carrier-v8.html (Abrufdatum 16. Mai 2017).

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] 07

402) [redacted]

403) *Dr. Köbele*, Protokoll-Nr. 33 I, S. 126; ohne explizitem Wissen zum Thema Carrier Sales, vgl. S. 148.

404) *Dr. Köbele*, Protokoll-Nr. 33 I, S. 140.

405) Näheres dazu in *Alster*, Protokoll-Nr. 30 II (Tgb.-Nr. 177/15 – GEHEIM), S. 11.

406) *Ricke*, Protokoll-Nr. 26 I, S. 112; [redacted]

407) *S. L.,* Protokoll-Nr. 26 I, S. 47.

ee) Vom Leerlaufen [redacted]

[redacted]

[redacted]

408) „Auf Grundlage der europarechtlichen Vorgaben und der Vorgaben des Bundesdatenschutzgesetzes führte die Deutsche Telekom bereits im Jahr 2004 den Privacy Code of Conduct als unternehmensinterne Regelung zum Datenschutz im Konzern ein. Der Privacy Code of Conduct regelt die internen Anforderungen an den Umgang mit personenbezogenen Daten weltweit einheitlich." (*Deutsche Telekom AG*, Datenschutzbericht 2009, S.30 ff., Anhang 3, § 17 ff. Privacy Code Of Conduct., der inhaltlich den Festlegungen von 2004 entsprechen dürfte). Heute lesen wir: „Datenschutz ist für uns nicht nur Pflicht, sondern ein besonders wichtiges Anliegen. Mit unserer weltweit agierenden Datenschutzorganisation ermöglichen wir, dass überall die gleichen hohen Standards für unsere Produkte und Services gelten.", https://www.telekom.com/de/verantwortung/datenschutz-und-datensicherheit/datenschutz; letzter Abruf 15. Mai 2017.

[redacted]

[redacted]

ff) Zusammenfassung

[redacted]

409) *Dr. Köbele*, Protokoll-Nr. 33 I, S. 128 ff.; [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

4. G 10-Anordnung als „Türöffner“

a) Rechtliche Überlegungen in BND und Kanzleramt

[redacted]

[redacted][411]

Um die Operation EIKONAL zusammen mit der NSA weiterbetreiben zu können, sah der BND den einzigen Ausweg darin, für diese Praxis eine G 10-Anordnung zumindest zum Schein zu erwirken. Der BND begann daraufhin im August 2004 erneut, die rechtliche Zulässigkeit einer Nutzung von Ausland-Ausland-Verkehren zu prüfen, die „zufällig" im Rahmen einer G 10-Maßnahme miterfasst würden. BND-Präsident *Hanning* drängte den Abteilungsleiter 6 im Kanzleramt, *Ernst Uhrlau*, eine Entscheidung zugunsten einer Zulässigkeit zu treffen. In einem Gesprächsvermerk, der nach der sog. Präsidentenrunde im Kanzleramt vom 17. August 2004 vom BND angefertigt wurde, heißt es:

> „Thema wurde bilateral mit AL6/BK aufgenommen. AL6/BK wird die Problematik nochmals in seiner Abteilung erörtern. Pr BND wies auf die besondere Bedeutung der Angelegenheit hin und unterstrich dabei, dass nach Auffassung des BND die Ableitung von Routineverkehren nicht vom G10-Gesetz erfasst werde und auch rechtspolitisch jeder Ausweitung der G 10-Kontrollen auf bisher nicht dem Gesetz unterliegende Verkehre strikt entgegengewirkt werden sollte."[412]

Das BND-Justiziariat (47A) verfasste schließlich Anfang September 2004 eine rechtliche Stellungnahme für Präsident *Hanning*, in der diese Rechtsauffassung niedergelegt

---

410) Aus Sicht des BND und der Bundesregierung ist nur die Kommunikation in Deutschland und von bzw. mit einem Teilnehmer in Deutschland von Artikel 10 GG geschützt sowie die Kommunikation von und mit Deutschen im Ausland, sofern sie nicht für eine ausländische juristische Person kommunizieren („Funktionsträgertheorie"; siehe hierzu Kapitel VIII.1.b) – Rechtswidrigkeit der BND-eigenen Selektoren.

411) Näheres dazu in eingestuften Akten in: MAT A BND-9/6 / BND-17/3 (Tgb.-Nr. 20/14 – STRENG GEHEIM, pauschal herabgestuft auf GEHEIM, nur zur Einsicht in der Geheimschutzstelle des Deutschen Bundestages), Anl. 05, Ordner 188, Bl. 62-66.

412) MAT A BND-17/3, Tgb.-Nr. 20/14 – STRENG GEHEIM, pauschal herabgestuft auf GEHEIM, nur zur Einsicht in der Geheimschutzstelle des Deutschen Bundestages), Anl. 10, Ordner 193, Bl. 55 (offen).

ist: Ausland-Ausland-Verkehre seien nicht von Artikel 10 GG geschützt. Sie fielen daher nicht unter das Artikel 10-Gesetz und könnten – auch wenn sie an einem G 10-Abgriff gewonnen würden – vom BND verwendet werden. Die in § 27 Abs. 2 Nr. 2 Telekommunikationsüberwachungsverordnung (TKÜV)[413] statuierte Löschungsverpflichtung für alle ausgeleiteten TK-Verkehre, die nicht von der entsprechenden G 10-Anordnung erfasst werden, gelte hier nicht.

Mit dieser rechtlichen Stellungnahme im Gepäck versuchte Präsident *Hanning*, das Kanzleramt von weiteren rechtlichen Prüfungen abzubringen. In einem BND-Schreiben an den Abteilungsleiter 2 vom 28. September 2004 wird über das Gespräch zwischen Hanning und Uhrlau berichtet,

> „[redacted]
>
> [redacted]“[414]

Ob und wenn ja welche Prüfungen und Erwägungen in den zuständigen Referaten der Abteilung 6 im Kanzleramt daraufhin stattfanden, erschließt sich aus den Akten nicht. Bei einer Besprechung im Kanzleramt am 20. Oktober 2004 unter der Leitung von *Uhrlau* zwischen Vertretern der Abteilung 2 des BND und hochrangigen Vertretern der Abteilung 6 des Kanzleramtes war jedenfalls die Frage der rechtlichen Zulässigkeit der Nutzung von Ausland-Ausland-Verkehren bei einem G 10-Abgriff kein Thema mehr. Hierbei ging es nur noch darum, die für die Operation EIKONAL „notwendige“ G 10-Anordnung erhalten. In dem Ergebnisvermerk der Besprechung ist festgehalten:

---

413) Bis 8. November 2005 war dies in Absatz 2 geregelt; in den Fassungen ab 9. November 2005 in Absatz 3.

414) MAT A BND-17/3, Tgb.-Nr. 20/14 – STRENG GEHEIM, pauschal herabgestuft auf GEHEIM, nur zur Einsicht in der Geheimschutzstelle des Deutschen Bundestages), Anl. 10, Ordner 193, Bl. 54 (VS-NfD).

> „– In Fragen der Behandlung bzw. Selektion leitungsvermittelter ‚Transit'-Verkehre sowie der Ableitung von ‚Routineverkehren' aus G 10 besteht kein Handlungsbedarf.
>
> Handlungsbedarf besteht hinsichtlich der Darlegung des Vorhabens zur Überwachung paketvermittelter Verkehre gegenüber [geschwärzt/TK-Unternehmen] und der G 10-Kommission. In der Diskussion wurden die Optionen ‚Erstellen eines Gutachtens durch BK' und ‚Herbeiführen eines förmlichen Beschlusses der G 10-Kommission ausgeschlossen'. Eine Änderung des G10-Gesetzes wäre nicht vermittelbar."[415]

Trotz des hohen Risikos, insbesondere bei der Erfassung von Internetverkehren hat das Kanzleramt auf ein Rechtsgutachten oder eine Befassung der G 10-Kommission mit den tatsächlichen Absichten hinsichtlich der „Routineverkehre" bewusst verzichtet. Stattdessen wurde vereinbart, einen „Probeantrag" bei der G 10-Kommission für die G 10-Erfassung zu stellen und der Kommission in einem Vortrag „den aktuellen Stand der technischen Erfassungsmöglichkeiten" zu präsentieren.[416]

Letztlich hatten BND und Kanzleramt damals erkannt, dass bereits kurz nach der Neuregelung im Artikel 10-Gesetz von Juni 2001, die eine Aufklärung von leitungsgebundenen Verkehren erst möglich gemacht hatte, eine neue Rechtsgrundlage erforderlich war, um weiterhin Ausland-Ausland-Verkehre im Zeitalter der IP-Verkehre erfassen zu können.

Den rechtsstaatlich gebotenen Weg einer Gesetzesänderung ist das Kanzleramt unter der Leitung von *Steinmeier* jedoch nicht gegangen. Der Zeuge *Uhrlau* verwies in seiner Aussage auf die damalige (rot-grüne) „Koalitionssituation".[417] Diese Schuldzuweisung lenkt von der Motivationslage auf Seiten des BND und Kanzleramtes ab, denn selbst nach weiteren zwei Großen Koalitionen und einer schwarz-gelben Koalition bedurfte

415) Unterrichtungsvorlage für AL6/BK vom 27. Oktober 2004, MAT A BND-17/3_Auszug_offen, Bl. 11-13 (12).

416) Unterrichtungsvorlage für AL6/BK vom 27. Oktober 2004, MAT A BND-17/3_Auszug_offen, Bl. 11-13 (12 f.).

417) *Uhrlau*, Protokoll-Nr. 81 I, S. 95.

es erst der Enthüllungen durch *Edward Snowden*, der Anhörungen von ehemaligen Bundesverfassungsrichtern als Sachverständige im Ausschuss und der öffentlichen Diskussion, dass die Bundesregierung und die sie tragenden Fraktionen von Union und SPD anerkannten, dass der BND für Ausland-Ausland-Erfassungen eine spezifische Rechtsgrundlage benötigt.

Den Äußerungen des damaligen BND-Präsidenten *Hanning* (s.o.) lässt sich entnehmen, dass eine Kontrolle der sog. Routineaufklärung, die mengenmäßig nach Aussagen der BND-Zeugen 90 bis 99 Prozent des Aufkommens ausmache, nicht gewünscht, ja sogar um jeden Preis vermieden werden sollte.[418] Der BND sollte ungestört im rechtsfreien und vor allem gänzlich unkontrollierten Raum weiterarbeiten können. Die mit der NSA vereinbarte Kooperation für den Kabelabgriff in Frankfurt am Main im Rahmen der Operation EIKONAL verstärkte den Druck, den BND notfalls auch rechtswidrig agieren zu lassen.

b) Nutzung von Ausland-Ausland-Verkehren aus G 10-Abgriffen unzulässig

aa) Fehlende Rechtsgrundlage

Das rechtliche Problem einer Zweckentfremdnung von G 10-Anordnungen für die Gewinnung von Daten aus reinen Auslands-Telekommunikationsverkehren war BND und Kanzleramt im Jahr 2004 voll bewusst. In der Abteilung 2 des BND wurden die verschiedenen Rechtsauffassungen klar benannt: Aus Sicht der Abteilung 2 beruhe die Miterfassung von Ausland-Ausland-Verkehren bei G 10-Maßnahmen auf § 1 Abs. 2 und § 3 BND-Gesetz i. V. m. § 8 Abs. 2 BVerfSchG. Nach der Gegenansicht sei das Artikel 10-Gesetz einschlägig, und insbesondere verlange § 27 Abs. 2 Nr. 2 TKÜV bei G 10-Maßnahmen die sog. Routineverkehre unmittelbar zu löschen.[419]

418) *Hanning,* Protokoll-Nr. 65, S. 28f.

419) Siehe hierzu detailliert: Unterrichtung des BND-Präsidenten vom 5. April 2004, MAT A BND-9/1 (Tgb.-Nr. 05/14 – STRENG GEHEIM, pauschal herabgestuft auf GEHEIM, nur zur Einsicht in der Geheimschutzstelle des Deutschen Bundestages), Anl. 01, Ordner 130, Bl. 49-51; MAT A BND-9/6 / BND-17/3, Tgb.-Nr. 20/14 – STRENG GEHEIM, pauschal herabgestuft auf GEHEIM, nur zur Einsicht in der Geheimschutzstelle des Deutschen Bundestages), Anl. 08, Ordner 191, Bl. 11; in der Neufassung der TKÜV, die am 9. November 2005 in Kraft trat, wird die Löschung in Absatz 3 Nr. 2 geregelt.

Die Ausleitung und Verwendung der Ausland-Ausland-Verkehre, die mithilfe einer G 10-Anordnung bei der *Telekom* erwirkt wurde, war rechtswidrig.

Für einen solchen Abgriff im Inland fehlte es an einer Rechtsgrundlage[420]. Der Verweis auf die Aufgabennorm in § 1 BND-Gesetz (Sammeln von Informationen über das Ausland) in Verbindung mit der Befugnis zur „heimlichen Beschaffung von Informationen" in § 3 BND-Gesetz, der wiederum auf Befugnisse aus § 8 Abs. 2 BVerfSchG verweist, kann eine spezifische Befugnisnorm für den BND nicht ersetzen. § 8 Abs. 2 BVerfSchG gestattet gerade keine strategische Fernmeldeaufklärung (die das BfV auch gar nicht durchführen darf) und auch keine anderweitige Überwachung der Telekommunikation. In Absatz 2 sind vielmehr Methoden, Gegenstände und Instrumente der heimlichen Informationsbeschaffung „wie de[r] Einsatz von Vertrauensleuten und Gewährspersonen, Observationen, Bild- und Tonaufzeichnungen, Tarnpapiere und Tarnkennzeichen" aufgelistet. Die Nichtanwendbarkeit von § 8 Abs. 2 BVerfSchG als Rechtsgrundlage für die strategische Fernmeldeaufklärung des BND ergibt sich auch daraus, dass Maßnahmen der Telekommunikations- und Postüberwachung in anderen Absätzen des § 8 BVerfSchG geregelt sind, wie beispielsweise die Bestandsdaten- und Verbindungsdatenauskunft bei TK-Anbietern im damaligen Absatz 8. In der Erfüllung des Zitiergebots (damaliger Absatz 12 des § 8), mit dem der Gesetzgeber in diesem Fall auf die Einschränkung des Grundrechts des Brief-, Post- und Fernmeldegeheimnisses (Artikel 10 des Grundgesetzes) hinweisen muss, werden nur die Absätze 6, 8, 9 und 11 genannt, nicht jedoch der Absatz 2.

§ 1 Abs. 2 und § 3 BND-Gesetz i. V. m. dem damaligen § 8 Abs. 2 BVerfSchG konnten daher keine Rechtsgrundlage für die Ausleitung von Ausland-Ausland-Verkehren im Rahmen von G 10-Anordnungen sein. Auch eine andere Befugnisnorm ist nicht ersichtlich und wurde vom BND auch nicht angeführt.

420) siehe zur Geltung von Artikel 10 GG auch bei der Ausland-Ausland-Aufklärung eingehend unter V.3.b)b)) EIKONAL Abgriff ohne G10-Anordnung

bb) Löschungspflicht für Ausland-Ausland-Telekommunikation nach TKÜV

Zum anderen hätte der BND Telekommunikationsverkehre, die nicht von der G 10-Anordnung umfasst sind, aufgrund von Bestimmungen in der TKÜV gar nicht erhalten dürfen.

In der TKÜV wird die technische und organisatorische Umsetzung von Maßnahmen zur Überwachung der Telekommunikation geregelt. Welche Maßnahmen dies sind, ist dort abschließend geregelt. In der damaligen bis 8. November 2005 geltenden Fassung waren dies in § 1 TKÜV die a) in den §§ 100a und 100b der Strafprozessordnung, b) in den §§ 3, 5 und 8 des Artikel 10-Gesetzes sowie c) in den §§ 23a bis 23f sowie §§ 45 und 46 des Zollfahndungsdienstgesetzes vorgesehenen Überwachungsmaßnahmen.[421] Überwachungsmaßnahmen aufgrund des BND-Gesetzes waren dort nicht genannt.

Aufgrund der damaligen TKÜV konnte daher kein TK-Anbieter verpflichtet werden, bestimmte Vorkehrungen und Maßnahmen zu treffen, um für den BND Telekommunikationsverkehre außerhalb von G 10-Anordnungen (hier insb. § 5 Artikel 10-Gesetz) auszuleiten. Erst als Folge der BND-Gesetzesänderung von Dezember 2016 ist in der aktualisierten TKÜV in § 1 die „Ausland-Ausland-Fernmeldeaufklärung“ des BND vom Inland aus ausdrücklich mit aufgenommen worden.[422]

Es fehlte damals nicht nur an einer Verpflichtung für den TK-Betreiber. Nach der Vorschrift in § 27 TKÜV (a. F.) durften dem BND auch keine über die in der G 10-Anordnung hinaus bezeichneten TK-Verkehre übermittelt werden.

In § 27 TKÜV (a. F.) wird der Umgang mit TK-Verkehren ausschließlich aus Maßnahmen des BND nach den §§ 5 (strategische Fernmeldeaufklärung) und 8 Artikel 10-Gesetz reglementiert. § 27 Abs. 2 TKÜV schreibt vor, wie die Geräte des BND, die für die Überwachungsmaßnahme eingesetzt werden, beschaffen sein müssen, um die

421) In späteren Fassungen wurden noch Maßnahmen im Landesrecht sowie in § 20l des Bundeskriminalamtgesetzes ergänzt.

422) Zum Zeitpunkt der Erstellung des Berichts lag der Entwurf vor: Bundesrats-Drucksache 243/17 vom 23. März 2017, Bundesrats-Drucksache 243/1/17 vom 7. Mai 2017; Einfügung von Maßnahmen in den §§ 6, 12 und 14 des neuen BND-Gesetzes.

ausgeleitete vollständige Kopie der Telekommunikation aus den in der G 10-Anordnung benannten Übertragungswegen (Strecken, z.B. das Glasfaserkabel von A nach B) noch in den Räumen des TK-Betreibers zu bearbeiten, *bevor* sie an den BND übermittelt wird. In den Nummern 1 und 2 heißt es:

> „1. die nach Absatz 1 bereitgestellte Kopie wird in der Weise bearbeitet, dass die Festlegung nach § 10 Abs. 4 Satz 3 des Artikel 10-Gesetzes eingehalten und die danach verbleibende Kopie an den Bundesnachrichtendienst nur insoweit weiterübermittelt wird, als sie Telekommunikation mit dem in der Anordnung nach § 10 Abs. 4 Satz 2 des Artikel 10-Gesetzes bezeichneten Gebiet enthält;
>
> 2. im Übrigen wird die Kopie gelöscht.“[423]

Das heißt, das BND-Gerät muss aus der Kopie zunächst die Datenmenge soweit reduzieren, dass der in der Anordnung benannte Anteil – dies dürfen max. 20 Prozent der auf der bezeichneten Strecke zur Verfügung stehenden Übertragungskapazität sein – übrig bleibt.[424] Von diesen Daten erhält der BND anschließend nur solche Telekommunikation, die mit einem der in der G 10-Anordnung genannten Staat oder einer genannten Region geführt wird.[425] Nach § 5 Artikel 10-Gesetz betrifft dies „internationale Telekommunikationsbeziehungen“. Damit sind solche gemeint, bei denen der eine Endpunkt *in Deutschland* und der andere Endpunkt in einem bestimmten Staat oder einer Region *außerhalb Deutschlands* liegt.[426] Reine Ausland-Ausland-Kommunikation, um die es dem BND nach eigenen Angaben bei EIKONAL ging, war davon nicht erfasst und durfte nicht an den BND übermittelt werden. Reine Auslandsverkehre waren zu löschen, wie § 27 Abs. 2 Nr. 2 TKÜV vorschrieb. Die Praxis des BND, sich aus einer Maßnahme nach § 5 Artikel 10-Gesetz weitere, nicht von der G 10-Anordnung umfasste TK-Verkehre übermitteln zu lassen, ist rechtswidrig.

---

423) Mit Inkrafttreten am 9. November 2005 findet sich die Vorschrift in Absatz 3 des § 27 TKÜV.

424) § 10 Abs. 4 Satz 3 Artikel 10-Gesetz.

425) § 10 Abs. 4 Satz 2 Artikel 10-Gesetz.

426) Vgl. *Droste*, Handbuch des Verfassungsschutzrechts, Stuttgart u. a. 2007, S. 351.

c) Täuschung der G 10-Kommission

aa) Vorgehen des BND

Seit der Entscheidung im Kanzleramt von Oktober 2004, wegen [redacted] nun Daten für die Operation EIKONAL verdeckt aus einer G 10-Maßnahme zu nutzen, traf der BND technische Vorbereitungen für den Abgriff bei der *Telekom* in Frankfurt am Main und für den Antrag der G 10-Maßmaßnahme nach § 5 Artikel 10-Gesetz. Dazu gehörte die Entwicklung eines sog. Separators, einer Soft- und Hardware, die die TK-Verkehre in vermeintlich G 10-geschützte und reine Auslandsverkehre trennen sollte. Außerdem wurde durch das BSI ein Erfassungsgerät für die G 10-Maßnahme „zertifiziert“, das letztlich auch für die Operation EIKONAL genutzt werden sollte.[427]

Die G 10-Anordnung für den Gefahrenbereich des internationalen Terrorismus, die verdeckt für die Operation EIKONAL genutzt werden sollte, genehmigte die G 10-Kommission am 20. Oktober 2005 – ohne dass die Kommission über die wahren Absichten des BND bzw. die Kooperation mit der NSA informiert worden war. Sie wusste nur, dass der BND auch erstmals paketvermittelte Verkehre bei der strategischen Fernmeldeaufklärung erfassen wollte. Die Anordnung wurde zunächst auf sechs Monate für einen Probebetrieb bewilligt. In dem Text der Anordnung, die im üblichen Verfahren vom Bundesministerium des Innern ergangen war, findet sich keinerlei Hinweis darauf, dass im Rahmen der G 10-Maßnahme auch anfallende reine Auslandskommunikation erfasst und genutzt werden, geschweige denn, dass sie in einer gemeinsamen Operation von BND und NSA verarbeitet bzw. Daten daraus an die NSA weitergeleitet werden sollten.[428]

427) siehe dazu unter V.5 – EIKONAL: Unzulängliche BSI-Prüfung

428) Die Anordnung und die Verlängerungen finden sich in eingestuften Unterlagen des Ausschusses in: MAT A BMI-11 (Tgb.-Nr. 44/14 – GEHEIM).

bb) Eigentliche Absichten des BND gegenüber der G 10-Kommission verschleiert

Am 21. Oktober 2005, einen Tag, nachdem die G 10-Anordnung „genehmigt“ worden war, verfasste der damalige Abteilungsleiter 2 *Breitfelder* eine Entscheidungsvorlage an Präsident *Hanning*. Unter dem Betreff „JSA“, also der gemeinsamen BND-NSA-Einheit *Joint SIGINT Activity* in Bad Aibling, in der die Daten aus der Operation EIKONAL bearbeitet wurden, berichtete der Abteilungsleiter 2 über den „erfolgreichen“ G 10-Antrag. In einer handschriftlichen Notiz auf dem Papier, das dem Ausschuss aus BND-Unterlagen vorgelegt wurde, ist angemerkt:

> „– [redacted]
>
> – [redacted]!
>
> [redacted]!
>
> [redacted].“[429]

Wer der Verfasser der Notiz aus dem BND war, konnte der Ausschuss nicht ermitteln. Die Notiz belegt, dass es sich bei der erwirkten G 10-Anordnung selbst aus Sicht des

429) MAT A BND-9/1, Tgb.-Nr. 05/14 – STRENG GEHEIM, pauschal herabgestuft auf GEHEIM, nur zur Einsicht in der Geheimschutzstelle des Deutschen Bundestages), Anl. 02, Ordner 131, Bl. 1-3; MAT A BND-9/6 / BND-17/3, Tgb.-Nr. 20/14 – STRENG GEHEIM, pauschal herabgestuft auf GEHEIM, nur zur Einsicht in der Geheimschutzstelle des Deutschen Bundestages), Anl. 05, Ordner 188, Bl. 67-69.

BND um einen „Türöffner“ für den Abgriff von Ausland-Ausland-Verkehren gehandelt hat. Aus dem Betreff „JSA“ und dem Inhalt der Notiz wird deutlich, dass es dem BND darum ging, mittels der G 10-Anordnung die Kooperationsvereinbarung mit der NSA in Bad Aibling zu erfüllen und den Anschein der Erfüllung von rechtlichen Voraussetzungen zu erzeugen, [redacted]

Auch aus den Aussagen der BND-Zeugen vor dem Ausschuss wird der eigentliche Zweck für die Beantragung der G 10-Anordnung, nämlich der Abgriff von reinen Auslandsverkehren für die Kooperation mit der NSA, deutlich.

Der Zeuge *Breitfelder* hat hierzu geäußert:

> „Paketvermittelt: Da sind wir dann auf die Idee gekommen und sagen: Pass auf mal, der Strom, der da durchläuft – wir wollen ja ohnehin nur Auslandsverkehre –, da können wir doch eine G-10-Anordnung anfragen. Wenn wir eine G-10-Anordnung haben, dann kommt uns auch der Routineverkehr mit rein. Da haben wir doch das, was wir wollen. – Das haben wir dann gemacht. Mit der G-10-Anordnung greift ja die Telekommunikations-Überwachungsverordnung, und da wird ja der Betreiber verpflichtet, uns den Zugang zu gewähren.“[430]

Dass die G 10-Kommission getäuscht werden sollte, bestätigte der Zeuge *Breitfelder* an anderer Stelle:

> „Ja, mein technischer Mitarbeiter, der mir ja gesagt hat, der Betreiber will uns nicht ranlassen. Dann habe ich das angesteuert über den Präsidenten und habe gesagt: Hier, der Betreiber lässt uns nicht ran; der braucht da irgendwas, Präsident. – Dann habe ich mitgekriegt: Irgendwann kam mein Techniker wieder und hat gesagt: Die schreiben jetzt einen Brief, und dann sehen wir mal weiter. – Und dann kam er wieder und hat gesagt nach einiger Zeit: Hat funktioniert. Wir müssen jetzt

430) *Breitfelder*, Protokoll-Nr. 28 I, S. 37.

> eine G 10-Anordung bewirken, und dann können wir da dran. – So ungefähr lief das ab.“[431]

Neben der Tatsache, die *Breitfelder* bestätigt, dass der Abgriff zunächst ohne G 10-Anordnung laufen sollte, wird auch an anderer Stelle deutlich, worum es dem BND primär ging:

> „Also, es ist ja nicht so, dass wir keine G 10 – – dass wir das G-10-Aufkommen nicht brauchen würden. Das war für uns schon auch wichtig. Das war also ein doppelter Nutzen. Wir hatten das G-10-Aufkommen, und wir hatten das Routineaufkommen, das uns die Verpflichtung erfüllen ließ gegenüber der NSA.“[432]

Hier wird explizit von „auch wichtig“ gesprochen und von doppeltem Nutzen. Dieser doppelte Nutzen diente der Erfüllung der Verpflichtungen gegenüber der NSA. Aus der Formulierung ergibt sich aber, dass diese Verpflichtungserfüllung nicht der „Beifang“ der Aktion war, sondern das primäre Ziel.

Auch indirekt hat der Zeuge *Breitfelder* bestätigt, dass die G 10-Kommission nicht umfassend informiert wurde:

> „Wir haben uns gesagt: Wenn du dazu gefragt wirst, sagst du die Wahrheit, und wenn du nicht gefragt wirst, dann sagst du auch nichts. Das war die allgemeine Haltung.“[433]

Dies passt zu der Antwort auf die Frage des Abgeordneten *von Notz*, warum eine G 10-Anordnung vermieden werden sollte. Darauf hat der Zeuge *Breitfelder* erwidert:

431) *Breitfelder*, Protokoll-Nr. 28 I, S. 55.

432) *Breitfelder*, Protokoll-Nr. 28 I, S. 63.

433) *Breitfelder*, Protokoll-Nr. 28 I, S. 60.

> „Das habe ich nie gesagt, dass wir sie vermeiden wollten. Ich habe nur gesagt: Wir brauchten sie, um in Frankfurt ans Kabel zu kommen.“[434]

Er hat später ergänzt:

> „Ja, das heißt doch nichts anderes, dass wir versucht haben, ganz, also ohne weitere Maßnahme, an das Kabel zu kommen, und dass der Betreiber uns gesagt hat: Nein, das geht so nicht. – So. Dann führe ich im Folgenden auf, welche Schritte erforderlich sind, erkläre das der NSA und – – Ja, das war‘s.“[435]

Die These, dass es bei der G 10-Anordnung für paketvermittelte Verkehre primär um die Abschöpfung der „Routineverkehre“ ging, wird durch die Aussage des damaligen Abteilungsleiters 6 im Kanzleramt, des Zeugen *Uhrlau*, gestützt:

> „Was eine Rolle gespielt hat bei G 10 und Routineverkehr: dass wir auf der sicheren Seite sind, wenn wir einen G 10-Antrag haben, in dem zwar viel Routine ist, aber nicht Gefahr laufen, dass wir dann plötzlich relevante Informationen bekommen, die eigentlich G-10-relevant sind, aber wegen eines fehlenden G-10-Antrages nicht hätten erfassen dürfen. Also deswegen Erfassung unter G 10, das ist der sinnvolle Ansatz, um auch bei ‚Routine, G 10 und Routine‘ dann trennen zu können.“[436]

Danach sei es dem BND in erster Linie um die Auslandsverkehre gegangen. Um aber dabei ggf. auftretende nachrichtendienstlich relevante G 10-geschützte Telekommunikation verarbeiten zu können, werde die G 10-Anordnung benötigt. Die G 10-Verkehre wären demnach nur „Beifang“.

---

434) *Breitfelder*, Protokoll-Nr. 28 I, S. 75.

435) *Breitfelder*, Protokoll-Nr. 28 I, S. 76 f.

436) *Uhrlau*, Protokoll-Nr. 53 I, S. 37.

Wie irrelevant der „Beifang“ aus den G 10-Verkehren letztlich über die gesamte Dauer der Operation EIKONAL für den BND war, zeigen auch die Anordnungen des BMI selbst. In ihnen werden auch bei jeder Verlängerung die „Ergebnisse“ des vorangegangenen Zeitraums präsentiert. Dem Ausschuss lagen die für EIKONAL genutzten G 10-Anordnungen für den Zeitraum November 2005 bis Anfang Januar 2008 vor. Als Output der Überwachung der paketvermittelten Telekommunikation enthielten aus Sicht der Auswertung des BND nur eine handvoll Fernmeldeverkehre „nachrichtendienstlich relevante Informationen zu Auslandssachverhalten“. Diese wurden ausschließlich im Zeitraum Mai bis Oktober 2006 festgestellt.[437] Im Ergebnis hatte die Maßnahme also null Relevanz für den BND. Mit anderen Worten war diese G 10-Maßnahme völlig untauglich, überflüssig und hätte schnellstmöglich eingestellt werden müssen. Die G 10-Maßnahme und damit auch die massenhaften Grundrechtseingriffe – denn zu Erfassungen kam es sehr wohl, wie auch in den öffentlichen Berichten des PKGr nachlesbar ist – waren ein von Anfang an geplanter „Beifang“. Die (vermeintliche) Auslandskommunikation war der Hauptfang.

Auch der Umstand, dass der BND schließlich eine G 10-Anordnung im Gefahrenbereich „Internationaler Terrorismus“ beantragte[438] und nicht, wie ursprünglich vorgeschlagen im Gefahrenbereich „Proliferation“,[439] zeigt, wie beliebig und zweitranging die eigentliche G 10-Anordnung war. Ziel war die Zugriffsmöglichkeit auf die Auslandsverkehre aus dem *Telekom*-Knoten für EIKONAL.

[redacted] Dies hätte voraussichtlich ein sofortiges Ende der Operation EIKONAL bedeutet.

437) Details siehe in: MAT A BMI-11 (Tgb.-Nr. 44/14 – GEHEIM).

438) Details siehe in: MAT A BMI-11 (Tgb.-Nr. 44/14 – GEHEIM).

439) Unterrichtungsvorlage für AL6/BK vom 27. Oktober 2004, MAT A BND-17/3_Auszug_offen, Bl. 11-13 (12).

cc) Sicht der G 10-Kommission

Nach der Aussage des langjährigen Vorsitzenden der G 10-Kommission, des Zeugen *de With*, war ihm bzw. der G 10-Kommission damals nicht bewusst, dass das eigentliche Ziel der G 10-Anordnung von Oktober 2005 der Abgriff von reinen Auslandsverkehren war. Auch von einer Kooperation des BND mit der NSA, bei der Daten aus einem Frankfurter Netzknoten der *Telekom* gemeinsam bearbeitet werden sollten, wusste der Zeuge de With nichts, sondern hat erst aus der Zeitung davon erfahren.[440] Ihm seien weder die Operation EIKONAL noch rechtliche Bedenken oder Diskussionen vor der Durchführung der Operation zu Ohren gekommen.[441]

Auf den Vorhalt der handschriftlichen Notiz auf der Präsidentenvorlage vom 21. Oktober 2005 nach der Sitzung der G 10-Kommission tags zuvor, bei der die G 10-Anordnung genehmigt worden war (s. o. unter bb) – Eigentliche Absichten des BND gegenüber der G 10-Kommission verschleiert), hat der Zeuge *de With* ausgesagt:

> „Ich kann mich nicht erinnern, dass jemals eine entsprechende Frage bzw. ein Hinweis an uns gegeben wurde mit dem Begriff „Türöffner" oder es geht nur darüber, sodass ein anderer Zweck erreicht werden sollte. Daran kann ich mich nicht erinnern."[442]

Angesprochen auch auf die spezielle Problematik der paketvermittelten Verkehre in der Notiz hat *de With* gesagt:

> Kann ich nicht verstehen, muss ich rundum sagen. Wenn uns oder wenn mir bewusst gewesen wäre, dass hier etwas vorgeschoben wird, um einen Zweck zu erreichen, dann hätten wir, ich jedenfalls, nie akzeptiert. Das sage ich jetzt als Sachverständiger, weil das ja keine

440) *de With* nannte den Artikel aus der *Süddeutschen Zeitung* vom 4. Oktober 2014, „Codewort Eikonal".

441) *de With*, Protokoll-Nr. 43 I, S. 109, 110.

442) *de With*, Protokoll-Nr. 43 II – Auszug offen, S. 8.

> Tatsache ist (…) Ich wundere mich über diesen Vermerk, kann ich nur rundum sagen.“[443]

In einer Unterrichtungsvorlage für BND-Präsident *Uhrlau* vom 26. Januar 2006[444] hatte der damalige Unterabteilungsleiter *Urmann* den Präsidenten über den Stand und die Risiken der Operation EIKONAL, inbesondere durch die Zweckentfremdung einer G 10-Anordnung informiert. Darin heißt es:

„[redacted]

443) *de With*, Protokoll-Nr. 43 II – Auszug offen, S. 8.

444) MAT A BND-9/1 (Tgb.-Nr. 05/14 – STRENG GEHEIM, pauschal herabgestuft auf GEHEIM, nur zur Einsicht in der Geheimschutzstelle des Deutschen Bundestages), Anl. 02, Ordner 131, Bl. 4-8.

[redacted].“

Auf den Vorhalt dieses Dokuments äußerte der ehemalige G 10-Kommissionsvorsitzende *de With*:

> „Ich habe schon gesagt: Das hätte ich so nicht hingenommen.“[445]

Der Zeuge *de With* bewertete ein Vorgehen unter Täuschung der G 10-Kommission als einen Missbrauch:

> „Also, wenn eine G 10-Anordnung im strategischen Bereich durch den BND benutzt wird, die nicht erforderlich wäre, nur um an den Server zu kommen, dann halte ich das für missbräuchlich.“[446]

> „Wenn das so ist, wenn das Vehikel nicht notwendig ist, sondern gebraucht wird, um das zu erreichen, wäre das ein Missbrauch gewesen – wenn es denn so wäre.“[447]

---

445) *de With*, Protokoll-Nr. 43 II – Auszug offen, S. 10.

446) *de With*, Protokoll-Nr. 43 II – Auszug offen, S. 11.

447) *de With*, Protokoll-Nr. 43 II – Auszug offen, S. 12..

d) Zusammenfassende Bewertung

Das Vorgehen des BND und des Kanzleramtes war in vielfacher Hinsicht unzulässig.

Der Abgriff von Ausland-Ausland-Verkehren bei der *Telekom* in Frankfurt am Main durch den BND war aufgrund fehlender Rechtsgrundlage rechtswidrig. Dies gilt unabhängig davon, ob es sich um leitungsvermittelte oder paketvermittelte Verkehre gehandelt hat.

BND und Kanzleramt haben dies erkannt, aber es unterlassen, das Problem gegenüber der G 10-Kommission, dem Parlamentarischen Kontrollgremium oder dem Gesetzgeber anzuzeigen, um eine Rechtsänderung herbeizuführen. Nach der Entscheidung des Bundesverfassungsgerichts von 1999 zur strategischen Fernmeldeaufklärung muss es BND und Kanzleramt klar gewesen sein, dass zumindest für Erfassungen des BND in Deutschland wegen der Betroffenheit des Fernmeldegeheimnisses aus Artikel 10 GG eine eigene Rechtsgrundlage erforderlich gewesen wäre.

Eine Rechtsänderung war auf Seiten des BND gar nicht gewollt, um so die Erfassung von „Routineverkehren“, wie sie der BND verharmlosend bezeichnet, in einem kontrollfreien Bereich ungestört weiterführen zu können.

Durch die Kooperationsvereinbarung mit der NSA, bei der es um das Geschäft US-Technik und Know-how gegen Daten aus dem *Telekom*-Knoten in Frankurt am Main ging, hat sich der BND derart abhängig gemacht, dass ein Aufrechterhalten der Zusammenarbeit um nahezu jeden Preis verfolgt wurde, auch unter Inkaufnahme extremer rechtlicher und politischer Risiken bis hin zu verfassungswidrigem Handeln durch Grundrechtsverstöße und einer massiven Beschädigung aller beteiligten staatlichen Instutionen [redacted]

BND und Bundeskanzleramt haben die G 10-Kommission vorsätzlich getäuscht. Den eigentlichen Anlass für die damalige G 10-Anordnung haben sie gegenüber der Kommission bewusst verschwiegen. Die G 10-Anordnung wurde als „Türöffner“ missbraucht, um an die eigentlich gewollten Auslandsverkehre für die Operation EIKONAL in Kooperation mit der NSA zu gelangen. Diese TK-Verkehre wurden dann jenseits des Rechts erfasst, verarbeitet und an die NSA übermittelt – sie wurden gerade nicht unter den besonderen Schutzstandards behandelt, die das Artikel 10-Gesetz vorsieht.

Der BND befürchtete bei Bekanntwerden der Operation EIKONAL und des täuschenden Vorgehens sogar ein Moratorium für die G 10-Erfassung insgesamt. Die handelnden Personen bis in die Spitze des BND wussten, was sie taten und riskierten. Es durfte bloß nichts rauskommen und öffentlich werden. Tarnen, Täuschen und Vertuschen war angesagt, denn die ganze Operation einschließlich der erschlichenen Scheinlegitimation durch die G 10-Kommission war unzulässig und rechtswidrig. Das hat die Beweisaufnahme zweifelsfrei ergeben. Die Vorsätzlichkeit des Vorgehens und das schlechte Gewissen des BND finden sich in den Akten mehrfach dokumentiert. Die rechtlichen Bedenken, die es im BND und Kanzleramt an verschiedenen Stellen auf der Arbeitsebene gab, wurden unter voller Kenntnis durch Entscheidungen des BND-Präsidenten *Hanning* und des Abteilungsleiters 6 im Kanzleramt *Uhrlau* vom Tisch gewischt, offensichtlich mit politischer Rückendeckung.

Die Operation wurde über Jahre trotz aller Bedenken und Befürchtungen fortgesetzt. Das Parlamentarische Kontrollgremium wurde über diese nicht informiert und durfte offensichtlich nichts erfahren. Die Handelnden blieben von jeder Konsequenz verschont, auch als die Operation offiziell bekannt und öffentlich im Untersuchungsausschuss sowie in den Medien breit erörtert wurde. Niemand wurde zur Rechenschaft gezogen. Es scheint, es waren zu viele informiert und involviert – oder irgendwer hat seine schützende Hand über sie gehalten.

5. EIKONAL: Unzulängliche BSI-Prüfung

Es ist dem BND im Zusammenwirken mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) gelungen, unter Umgehung und Verletzung der gesetzlichen Regelungen eine Erfassungstechnik zu zertifizieren und für die Operation EIKONAL zum Einsatz zu bringen, die das Telekommunikationsgeheimnis und die Grundrechte der betroffenen Bürger_innen planmäßig verletzt. Es ist deutlich geworden, dass die zum damaligen Zeitpunkt maßgeblichen Vorschriften umgangen wurden. Angesichts der gleichzeitigen Täuschung der G 10-Kommission ist davon auszugehen, dass dies planmäßig und mit vollem Wissen der Rechtswidrigkeit erfolgte.

a) Prüfungsansatz des BSI

Der BND hatte sich entschlossen, für die Ausleitung und Erfassung paketvermittelter Kommunikationsverkehre eine G 10-Anordnung einzuholen, um verdeckt aus dem Abgriff bei der *Deutschen Telekom AG* Auslandsverkehre für die Operation EIKONAL auszuleiten.[448] Am Übergabepunkt der *Telekom* sollten mit dem sogenannten „Front-end-Separator“ unmittelbar die G 10-Verkehre von den vermeintlich ungeschützten Ausland-Ausland-Verkehren getrennt werden. Für dieses Erfassungsgerät war eine Zertifizierung durch das BSI erforderlich.

Die Zertifizierung des vom BND im Rahmen der Operation EIKONAL in Frankfurt a. M. eingesetzten Systems durch das BSI erfolgte im Prüfungszeitraum Juli 2005 – Oktober 2005 und wurde mit dem „[redacted]“ vom 13. Oktober 2005 abgeschlossen.[449] Prüfer war der vom Ausschuss vernommene Zeuge *Martin Golke*. Prüfgrundlage bildeten die fünf Kriterien aus § 27 Abs. 2 TKÜV Nr. 1-4 (i. d. F. von 2002).[450] Die Prüfung selbst erfolgte unter Laborbedingungen in Räumlichkeiten des BND. Im Prüfbericht heißt es dazu:

> „[redacted]“[451]

Der Zeuge *Golke* hat die Prüfung in seinem Eingangsstatement anlässlich seiner Vernehmung durch den Ausschuss wie folgt dargestellt:

> „Um den speziellen Anforderungen der TKÜV zu genügen, wurde damals ein eigenes, sich daran orientierendes Prüfverfahren entwickelt. […] Wenn Sie jetzt mal meinen Prüfbericht zur Hand nehmen, sehen

448) Siehe hierzu Abschnitt V.4 – EIKONAL G10-Anordnung als „Türöffner“.

449) Prüfbericht des BSI vom 13. Oktober 2005, MAT A BSI-8a, Bl. 9 ff. (VS-NfD).

450) Entspricht § 27 Abs. 3 Nr. 1-4 TKÜV (i. d. F. von 2005).

451) Prüfbericht des BSI vom 13. Oktober 2005, MAT A BSI-8a, Bl. 11 (VS-NfD).

> Sie, wie er strukturiert ist und wie ich die Prüfung angegangen bin. Ich habe fünf einzelne Zertifizierungspunkte aus § 27 TKÜV identifiziert und entsprechend interpretiert.“[452]

Wie der Zeuge *Golke* ferner aussagte, wurde die Funktionsweise des technischen Systems in Hinsicht „auf die Papierlage geprüft“[453]. Es handelte sich generell um eine Prüfung auf Schlüssigkeit, bei der eine separate Überprüfung der Hard- und Software als solche nicht erfolgte.[454] Diese Unterlassung bewerten wir als einen grundsätzlichen Mangel, zumal laut der Zeugenaussage *Golkes* BSI-Zertifizierungen nach § 27 Abs. 2 TKÜV Nr. 5 (i. d. F. von 2002)[455] durchgängig keiner gesonderten Hardware- und Softwareprüfung unterliegen.[456] Im konkreten Fall schwerwiegender allerdings ist, dass die Zertifizierung des Erfassungs- und Verarbeitungssystems selbst auf Basis der Ergebnisse der Schlüssigkeitsprüfung nicht hätte erteilt werden dürfen.

Ausweislich des Prüfberichts konnten lediglich die Kriterien „Verhinderung von Fernzugriffen“[457] und „Zugriffskontrolle“[458] durch technische oder räumlich-technische Komponenten umgesetzt werden. Für die drei weiteren, besonders grundrechtsrelevanten Prüfkriterien „Begrenzung der Region“[459], „Anteilreduktion des Gesamtverkehrs“[460] und „Löschung der nicht benötigten Überwachungsdaten“[461], galt das nicht.

---

452) *Golke*, Protokoll-Nr. 33 I, S. 7.

453) *Golke*, Protokoll-Nr. 33 I, S. 44.

454) *Golke*, Protokoll-Nr. 33 I, S. 24 u. 30.

455) Entspricht § 27 Abs. 3 Nr. 5 TKÜV (i. d. F. von 2005).

456) *Golke*, Protokoll-Nr. 33 I, S. 24 u. 38.

457) § 27 Abs. 2 Nr. 3 TKÜV (i. d. F. von 2002).

458) § 27 Abs. 2 Nr. 4 TKÜV (i. d. F. von 2002).

459) § 27 Abs. 2 Nr. 1 TKÜV (i. d. F. von 2002) i. V. m. § 10 Abs. 4 Satz 3 Artikel 10-Gesetz.

460) § 27 Abs. 2 Nr. 1 TKÜV (i. d. F. von 2002) i. V. m. § 10 Abs. 4 Satz 2 Artikel 10-Gesetz.

461) § 27 Abs. 2 Nr. 2 TKÜV (i. d. F. von 2002).

b) Fehlerhafte Prüfkriterien durch das BSI: Die 20 %-Regel

In der damals maßgeblichen Vorschrift des § 27 Abs. 2 Telekommunikationsüberwachungsverordnung (TKÜV – a. F.) wurden die Anforderungen an die technischen Geräte des BND für die strategische Fernmeldeaufklärung genau festgelegt. Allerdings ergibt der Prüfbericht ein von diesen Vorgaben abweichendes Prüfverfahren. So setzte der Zeuge *Golke* als erste Verarbeitungsstufe die regionale Begrenzung der TK-Verkehre an. Tatsächlich ergibt sich aber aus § 27 Abs. 2 Nr. 1 TKÜV (a. F.), dass zuallererst der Datenstrom vor Übergabe an den BND um 80 Prozent zu reduzieren ist. Denn zur Verarbeitung stehen lediglich 20 Prozent der übermittelten Telekommunikationsdaten zur Verfügung. Schon an dieser Stelle hätte die Prüfung des Separators beendet werden müssen, weil die gesetzlichen Anforderungen nicht eingehalten waren.

Dies galt insbesondere auch deshalb, weil anlässlich der BSI-Prüfung festgestellt wurde, dass diese Anteilsreduktion erst als dritter Schritt erfolgte und zudem gar nicht durch das Erfassungsgerät selbst geleistet wird. *Golke* hielt in seinem Bericht fett gedruckt fest:

> „[redacted][462]

Diese wurde vielmehr den Mitarbeitern des BND überlassen. Dazu hat der Zeuge *Golke* in seinem Prüfbericht festgehalten:

> „Diese Anforderung [Anteilreduktion des Gesamtverkehrs AF2] wurde nicht mit IT-Maßnahmen umgesetzt. Dies wurde so begründet, dass der Gesamtverkehr aller Auslandsverbindungen weitaus größer ist, als mit den vorhanden[en] Mitteln abgreif- und verarbeitbar. Da die 20%-Regel sich an diesem Gesamtverkehr und nicht an dem bei einem bestimmten TK-Provider lokal abgreifbaren Verkehrsaufkommen

462) Prüfbericht des BSI vom 13. Oktober 2005, MAT A BSI-8a, Bl. 13 (VS-NfD).

> orientiert, kann sie auch ohne weiteres mit anderen Maßnahmen eingehalten werden.“[463]

Diese Auffassung widerspricht der gesetzlichen Regelung. Ihre Anwendung hat nämlich zur Folge, dass der BND durch Einholen einer Vielzahl von G 10-Anordnungen den ihm zur Verfügung stehenden Anteil entgegen den Vorgaben des Gesetzgebers manipulieren und künstlich erhöhen kann. Dem Wortlaut der § 5 Artikel 10-Gesetz und § 27 Abs. 2 TKÜV (a. F.) ist zu entnehmen, dass sich der für die Verarbeitung durch den BND zu reduzierende Datenanteil immer auf die konkret erfasste Kommunikationsleitung bezieht. Die Auffassung, dass sich der reduzierte Anteil beispielsweise im Verhältnis zur Datenmenge aller internationalen Telekommunikationsverkehre von und nach Deutschland oder auch nur solcher von der *Deutschen Telekom AG* als hier verpflichtetem Unternehmen berechnet, findet sich dort nicht. Eine solche Auffassung – die der Zeuge *Golke* für das BSI akzeptierte – führte letztlich dazu, dass der BND mit Einsatz des Separators rechtswidrig einen „full take“ der betroffenen Übertragungsleitungen verarbeiten konnte.

Es ist davon auszugehen, dass der BND solcherart rechtswidrig zertifizierte Geräte in der Folgezeit auch an anderer Stelle einsetzte und damit seit Jahren über die gesetzlichen Grenzen hinaus rechtswidrig Telekommunikationsdaten erfasst und verarbeitet.

Zur Umsetzung der technisch nicht implementierten Anteilsreduktion des zu überwachenden Gesamtverkehrs auf maximal 20 Prozent empfahl *Golke* einen ‚[redacted] Darin folgte er, wie dem Prüfbericht zu entnehmen ist, den Darlegungen des BND in der Klärung technischer Fragen und zugleich dessen Gesetzesinterpretation. Demnach sei § 10 Abs. 4 Satz 3 Artikel 10-Gesetz nicht streckenbezogen auf die einer

463) Prüfbericht des BSI vom 13. Oktober 2005, MAT A BSI-8a, Bl. 14 f. (VS-NfD), Vorhalt in Protokoll-Nr. 33 I, S. 66.

464) Prüfbericht des BSI vom 13. Oktober 2005, MAT A BSI-8a, Bl. 17 (VS-NfD).

Beschränkung unterliegenden Übertragungswege auszulegen, sondern auf den ‚[redacted], der ‚[redacted].“[465]

Ob dies tatsächlich so ist, musste *Golke* dem BND glauben, Belege hatte er nicht:

> „Die machen Sachen, und ich muss gucken: Ist das noch so? – Hier haben sie das so gesagt. Diese 20 Prozent, das sind ja riesige Datenraten. Dieses Internet, das ist ja – – Da muss man mal gucken, wie viel die überhaupt – – Mir wurde immer gesagt, die können maximal 5 Prozent sowieso nur auf – –“[466]

c) Begrenzung der Region mittels IP-Adressen unzureichend

Das BSI hat sehr wohl erkannt, dass die nach dem Artikel 10-Gestez und der G 10-Anordnung vorgeschriebene Begrenzung des Datenstroms auf die angeordneten Regionen (d. h. der Telekommunikationsbeziehungen mit bestimmten Ländern und Regionen) bei paketvermittleten Verkehren problematisch und mittels einer Auswahl nach IP-Adressen, wie es das BND-Gerät vorsah, nur ungenau ist.

Entsprechend heißt es auf Basis der technischen Schlüssigkeitsbetrachtung unter „Begrenzung der Region“:

> ‚[redacted][467]

---

465) Prüfbericht des BSI vom 13. Oktober 2005, MAT A BSI-8a, Bl. 14 (VS-NfD).

466) *Golke*, Protokoll-Nr. 33 I, S. 60.

467) Prüfbericht des BSI vom 13. Oktober 2005, MAT A BSI-8a, Bl. 12 (VS-NfD).

Trotz der „[redacted]“[468] der Gerätschaften – und das nicht nur für die Begrenzung der Regionen – bescheinigte das BSI ein positives Prüfergebnis. Prüfer *Golke* empfahl zur Begrenzung der Region, das *Hilfsmittel* IP-Adressräume aus den RIR-Datenbanken „[redacted]“.[469] Dabei war ihm, wie seiner Vernehmung mittelbar zu entnehmen ist, bewusst, dass dieses Verfahren unzureichend ist und zu rechtswidrigen Eingriffen in die Kommunikationsrechte von Grundrechtsträgern führen kann. Gleichwohl rechtfertigte er sich, indem er nicht die Legalität des Mittels, sondern die Legitimität des Zwecks als Ausgangspunkt seiner Prüfhandlung betrachtete und auf diese Weise die technische Zertifizierung in eine entgegenkommende Konformitätsbewertung überführte. In seiner Vernehmung äußerte *Golke* zum Aspekt der grundrechtsbezogen unzureichenden Trennschärfe von IP-Adressen:

> „Und bei IP-Adressen ist es natürlich auch nicht – – Da können Sie jetzt nicht wie bei einer Telefonnummer gucken: Ist das ein Deutscher? Hat der einen deutschen Pass, ja oder nein? – Das ist bei einer IP-Adresse – die werden ja auch dynamisch vergeben teilweise – natürlich in der Tat eine Problematik. Wobei ich da jetzt nicht von einem 100-Prozent-Ansatz ausgehen kann, weil dann müsste ich ja wieder – – Dann wäre ich wieder die Brechstange, um dem BND zu sagen: Du darfst überhaupt nicht arbeiten. – Ich meine, dann muss der Gesetzgeber auch seine Konsequenzen ziehen und – was weiß ich – den BND verbieten oder so etwas. Aber ich bin nicht die Brechstange dafür.“[470]

Ausgehend von der Unschärfe der Zuordnung anhand von überwiegend dynamischen IP-Adressen, der Nutzung von Anonymisierungsdiensten und VPN war auch insoweit die Zertifizierung unzulänglich und damit rechtswidrig.

468) Prüfbericht des BSI vom 13. Oktober 2005, MAT A BSI-8a, Bl. 16 (VS-NfD).

469) Prüfbericht des BSI vom 13. Oktober 2005, MAT A BSI-8a, Bl. 17 (VS-NfD).

470) *Golke*, Protokoll-Nr. 33 I, S. 57.

d) Keine hinreichende Prüfung der Löschungspflicht

Verarbeitungssysteme des BND für vermeintlich reine Auslandsverkehre hat das BSI bei seiner Prüfung im Jahr 2005 nicht und auch sonst in keiner Weise betrachtet. Das ist insofern dem BSI nicht vorwerfbar, da es hierfür auch keine rechtlichen Vorschriften gab und daher solche TK-Verkehre ohnehin nicht ausgeleitet werden durften. Dies hat der BSI-Prüfer *Golke* jedoch verkannt. Im BSI-Prüfbericht heißt es dazu:

> „[redacted]“[471]

Eine derartige Unterscheidung lässt sich § 27 Abs. 2 TKÜV (a. F.) gar nicht entnehmen. Dort heißt es vielmehr, dass die Daten „im Übrigen“, also die jenseits der gesetzlichen Ermächtigung und der G 10-Anordnung erfassten Daten, zu löschen sind.[472] Eine Löschungspflicht hat der Zeuge *Golke* lediglich für sogenannten „Müll“ bzw. TK-Verkehre von außerhalb der angeordneten Regionen für notwendig erachtet. Die BSI-Zertifizierung war daher auch in diesem Punkt fehlerhaft und rechtswidrig. Das vom BND zum Einsatz vorgesehene System hätte daraufhin geprüft werden müssen, dass es sämtliche Daten, die über die G 10-Anordnung hinausgehen – also den sog. Routineverkehr –, unwiederbringlich löscht.

e) BSI-Prüfung im Ergebnis rechtswidrig

Im Ergebnis steht eine im Hinblick auf die grundrechtsrelevanten Aspekte unzulängliche Prüfung des Erfassungs- und Verarbeitungssystems für IP-Verkehre. Allerdings ist diese nicht allein individuellen Unzulänglichkeiten zuzuschreiben. Da der Prüfbe-

---

471) Prüfbericht des BSI vom 13. Oktober 2005, MAT A BSI-8a, Bl. 11 (VS-NfD).

472) Vgl. Abschnitt V.4.b)bb) – Löschungspflicht für Ausland-Ausland-Kommunikation nach TKÜV.

richt nach den Angaben des Zeugen *Golke* auch vom „Referatsleiter, Fachbereichsleiter und Abteilungsleiter und […] von der Beratung“[473] unterschrieben wurde, muss vielmehr von einem systematischen Versagen des BSI gesprochen werden. Dort wurde dem vom BND zur Zertifizierung vorgelegten Erfassungs- und Verarbeitungssystem für paketvermittelte Verkehre eine G 10-Konformität bescheinigt, die – selbst ausweislich des Prüfberichts – nicht bestand.

Es ist festzuhalten, dass die für das Erfassungssystem durch den Zeugen *Golke* im Auftrag des BSI erteilte Zertifizierung fehlerhaft und rechtswidrig war. Sie ermöglichte dem BND unter Verletzung der gesetzlichen Vorschriften einen „full take“ der erfassten Übertragungsleitungen und eine unkontrollierte Verarbeitung angeblich ungeschützter reiner Auslandsverkehre. Dass es dabei zu Eingriffen in auch nach Auffassung des BND geschützte Telekommunikationsverkehre gekommen ist, muss angesichts der Fehlerhaftigkeit der Zuordnung bspw. anhand von IP-Adressen[474] vorausgesetzt werden.

Ob, wie vom BND-Zeugen *A. S.* behauptet, vom BSI neben dem „Separator“ tatsächlich das „Verarbeitungssystem“ (welche Systeme dies auch umfassen mag) und der „DAFIS-Filter“ hinreichend geprüft wurden,[475] muss bezweifelt werden. Aus dem BSI-Prüfbericht vom 13. Oktober 2015 geht dies jedenfalls nicht hervor.

6. EIKONAL: Der Tausch „Technik gegen Daten“

Die Befassung mit der Operation EIKONAL hat gezeigt, dass der BND niemals eine derartige Kooperation mit der NSA hätte eingehen dürfen. Die Zusage gegenüber dem US-Dienst über die Teilhabe an Daten aus einem Abgriff an Glasfaserkabeln in Deutschland war ein schwerer Fehler und hätte nicht gegeben werden dürfen. Schon der Ansatz, aber auch die Art und Weise der Kooperation mit einem technisch weit überlegenen Partnerdienst führten zu schwerwiegenden Rechtsverletzungen bis hin zu Grundrechtsverstößen. Bereits mit Filtersystemen, die selbst aus Sicht des BND

473) *Golke*, Protokoll-Nr. 33 I, S. 64.

474) Vgl. Sachverständigengutachten *von Kay Rechthien*, MAT A SV-13/3, S. 13 f.

475) Vgl. im Feststellungsteil unter F.IV.3.c) – aaa) Das sogenannte Erfassungs- und Verarbeitungssystem EVN G10 III.

nicht zuverlässig funktionierten, hätte die Operation EIKONAL nicht betrieben werden dürfen.

a) Black Boxes: US-Technik gegen Daten

BND und Kanzleramt betonen bei jeder Gelegenheit, im Geheimdienstgeschäft gehe es immer um ein do ut des. Bei der Kooperation in Bad Aibling und bei EIKONAL war dies „ein Tauschgeschäft – Technik gegen Daten."[476] Um bei der Überwachung des Internetverkehrs mithalten zu können und die dafür notwendige NSA-Technik zu erhalten, ging der BND mit EIKONAL eine Kooperation ein, die er letztlich nicht mehr beherrschte und daher abbrechen musste.

Aus der Beweisaufnahme wissen wir: Die technischen Risiken, aber auch die rechtlichen und politischen Risiken, kannte der BND von Anfang an genau. An eine tatsächliche volle Kontrolle durch den BND glaubte zu Beginn der Kooperation nicht einmal der deutsche Dienst selbst. Aus den Unterlagen geht hervor, dass er befürchtete, nicht mehr Herr des Verfahrens zu sein. Vor allem die technische Unterlegenheit des BND war ein Problem, selbst wenn die NSA zusicherte, sich an deutsches Recht zu halten (was sie letztlich nicht tat, wie die NSA-Selektoren-Problematik und Spionage-Vorfälle zeigten).

Dabei war der BND durchaus misstrauisch gegenüber der NSA. Der damalige Abteilungsleiter 6, der Zeuge *Breitfelder*, sagte dies in seiner Vernehmung sehr offen auf die Frage, ob damals die Befürchtung bestand, dass sich die NSA ohne Kenntnis des BND Zugang zu Kabeln verschaffen wollte oder könne:

> „Also Kenntnis mit Sicherheit nicht, aber wenn Sie uns damals gefragt hätten, dann hätten wir gesagt: Wir gehen davon aus, dass die das machen."[477]

476) U. a. *W. K.*, Protokoll-Nr. 22 I, S. 25.

477) *Breitfelder*, Protokoll-Nr. 30 II – Auszug offen, S. 74.

Wegen des Misstrauens wurde unter Beteiligung des damaligen BND-Präsidenten *Hanning* festgelegt, dass keine „Black Boxes“ der NSA eingesetzt werden sollen,[478] sondern nur Systeme mit offengelegtem Quellcode. Damit der BND nachvollziehen könnte, was das System tut und dass es bspw. keine Hintertüren hat. Die NSA ließ sich offenbar nicht darauf ein. Den Akten ist jedenfalls nicht zu entnehmen, dass dem BND der Quellcode der genutzten NSA-Systeme vorlag. Der ehemalige Leiter der Joint SIGINT Activity (JSA) in Bad Aibling hat dies sogar ausdrücklich verneint.[479] Bei einer späteren Untersuchung der bei EIKONAL genutzten Systeme durch eine Projektgruppe im Jahr 2007 stellte sich heraus, dass der BND zum Teil tatsächlich gar nicht wusste, wie die eingesetzte NSA-Hard- und Software genau funktionierte und vor allem nicht, was sich bei Aktualisierungen veränderte.[480] Eine essentielle Vorbedingung des BND war somit nicht erfüllt worden.

b) „Kontrollsystem“ und „Stockholm-Syndrom“

Das Misstrauen gegenüber der NSA war auch berechtigt. So wurde dem BND im Verlauf der Kooperation bewusst, dass die NSA-Systeme tatsächlich „Hintertüren“ haben, mit denen Daten umgeleitet oder abgezweigt werden könnten.[481]

Der BND wusste oder ahnte zumindest – so legen es die Akten aus der Frühphase der Kooperation nahe –, dass die NSA bevorzugt selbst am Frankfurter Netzknoten die Daten erfasst hätte, ohne Umweg über den BND. Die NSA war auch sehr an den Netzwerkdaten insbesondere der *Deutschen Telekom* interessiert, bei der der Datenabgriff für die Operation EIKONAL schließlich stattgefunden hat. Diese Daten benötigt man u. a., um den Abgriffspunkt für Internetverkehre auszuwählen.

---

478) So auch *Breitfelder*, Protokoll-Nr. 24 I, S. 38.

479) *T. B.*, Protokoll-Nr. 20 I, S. 37 f.

480) Genaueres dazu in eingestuften Akten: Dokumentation GRANAT vom 2. August 2007 (sog. Schwachstellenbericht), MAT A BND-9/2 (Tgb.-Nr. 15/14 – STRENG GEHEIM, pauschal herabgestuft auf GEHEIM, nur zur Einsicht in der Geheimschutzstelle des Deutschen Bundestages), Anl. 01, Ordner 165, Bl. 37-175.

481) Details nur in eingestuften Akten, bspw. MAT A BND-27/6 (Tgb.-Nr. 217/15 – GEHEIM), Anl. 06, Ordner 441, Bl. 323, 325 sowie auch im genannten „Schwachstellenbericht“.

Der bereits erwähnte *EADS/Eurocopter*-Vorfall aus dem Jahr 2005/2006, bei dem die NSA Telefonnummern dieser Firmen in der JSA in Bad Aibling eingesteuert hatte, zeigte dem BND schließlich schwarz auf weiß, dass es keinen Anlass gab, der NSA leichtfertig zu vertrauen.

Möglicherweise in Folge dessen wurde vom BND im Februar 2006 heimlich ein „Kontrollsystem" an der Erfassungsstelle in Frankfurt am Main installiert, um alle Verkehrsdaten der erfassten Kommunikation in der BND-Zentrale zu sichern. Gegenüber der JSA in Bad Aibling, und damit auch gegenüber den dortigen BND-Mitarbeiter_innen, wurde die Existenz dieser Überwachungseinrichtung bewusst verschwiegen. Nur eine Handvoll Mitarbeiter_innen in der Zentrale in Pullach wussten davon. Der Zeuge *W. K.*, damals Sachgebietsleiter, hat dazu ausgesagt, dass das Kontrollsystem dazu gedient habe zu prüfen, ob tatsächlich nur mit solchen Selektoren Telekommunikation erfasst wurde, die auch vom BND freigegeben worden waren.[482] Offenbar bestand der Verdacht, dass am BND vorbei Suchbegriffe in die Erfassungssysteme eingeschleust werden oder anderweitig Kommunikationsdaten erfasst werden können.

Wie eine Ironie der Geschichte wirkt dann am Ende, dass der BND durch mangelhafte Prüfung der NSA-Selektoren selbst tausende unzulässige Suchbegriffe in die Erfassugssysteme eingestellt hat.[483]

Die BND-Mitarbeiter_innen in der JSA in Bad Aibling sahen sich seitens der Zentrale in Pullach dem Vorwurf ausgesetzt, sie seien „amerikanisiert".[484] Was wohl soviel bedeuten sollte, dass sie kritiklos mit den NSA-Mitarbeiter_innen zusammenarbeiteten. In diesem Zusammenhang fiel auch der Begriff „Stockholm-Sydrom". Das dadurch gezeichnete Bild beschreibt zutreffend die problematische Konstellation in der JSA.

Die JSA – mit Arbeitssprache Englisch – war vom BND als Sachgebiet mit NSA- und BND-Mitarbeiter_innen unter einem BND-Mitarbeiter als Leiter und einem der NSA als

482) *W. K.*, Protokoll-Nr. 48 I, S. 96 f.; zu Details des Kontrollsystems hat sich *W. K.* nur in eingestufter Sitzung geäußert, Protokoll-Nr. 35 II (Tgb.-Nr. 180/15 – GEHEIM), S. 59-64; an Ergebnisse des Kontrollsystems konnte sich der Zeuge *W. K.* nicht mehr erinnern, Protokoll-Nr. 35 II – Auszug offen, S. 62 f.

483) Siehe hierzu unter Kapitel V.8. – Verstöße bei der Verwendung von NSA-Selektoren.

484) Siehe hierzu den Vorhalt des Abgeordneten *Konstantin von Notz*, Protokoll-Nr. 39 II – Auszug offen, S. 54.

Stellvertreter aufgestellt. Sie war so organisiert, dass die NSA-Mitarbeiter_innen sich darin prinzipiell frei bewegen konnten, auch wenn ihnen „pärchenweise" Aufgaben zugeteilt waren. Das von BND-Zeug_innen beschworene Vier-Augen-Prinzip war reine Fiktion. Der Zeuge *T. B.*, von 2003 bis 2007 Leiter der JSA, räumte ein, dass die Mitarbeiter_innen der NSA auch durchaus selbständig und unkontrolliert arbeiteten:

> „weil ich bestimmte Aufgaben habe, und wenn er entsprechend ein Update einspielt, dann muss ich nicht daneben einen Zweiten sitzen haben, der auch schaut: Was läuft jetzt über den Bildschirm runter?"[485]

Zwar seien angeblich alle „Daten-Ausgänge" des gemeinsamen Sachgebiets JSA zur NSA vom BND kontrolliert worden. Datenabflüsse mittels Speichermedien wie USB-Sticks konnte der ehemalige JSA-Leiter jedoch nicht ausschließen.[486]

Von US-Seite wurden sehr bald Ergebnisse aus der gemeinsamen Kooperation erwartet. Immerhin hatte die NSA viel Technik bzw. Geld in die Operation EIKONAL gesteckt. Anhand der Unterlagen kommen wir zu der begründeten Einschätzung, dass es der NSA vor allem, wenn nicht sogar ausschließlich in der Kooperation um die Daten aus dem Kabelabgriff bei der *Telekom* ging. Die NSA lobte die Operation EIKONAL als „Kronjuwel der strategischen Kooperation" mit dem BND.[487] Der Betrieb der Satellitenerfassungsstelle in Bad Aibling war nur ein willkommener Beifang und diente gleichzeitig dem Verdecken des Kabelabgriffs. Entsprechend hoch war der Druck auf den BND, trotz schlecht funktionierender „G 10-Filter" Daten aus Frankfurt zu liefern.

c) G 10-Filter-Desaster

Das Filter-Problem zieht sich wie ein roter Faden durch die Operation EIKONAL und soll schlussendlich auch zu deren Abbruch geführt haben. Bei Beginn der Operation existierte gar kein Filter, um die erfasste Telekommunikation um solche von Deutschen bzw. aus oder nach Deutschland – sog. G 10-geschützte Verkehre – zu bereinigen.

---

485) *T. B.*, Protokoll-Nr. 20 I, S. 39.

486) *T. B.*, Protokoll-Nr. 20 I, S. 39.

487) Zitiert nach *Süddeutsche Zeitung* vom 4. Oktober 2014, „Codewort Eikonal" „ http://www.sueddeutsche.de/politik/geheimdienste-codewort-eikonal-der-albtraum-der-bundesregierung-1.2157432..

Das bedeutet, der BND begann eine Kooperation, bei der der NSA Daten aus einem deutschen Netzknoten versprochen worden waren, in denen unweigerlich Kommunikation von Deutschen enthalten sein würde – ohne eine Filtermöglichkeit. Eine unter diesen Umständen begonnene Operation nimmt Grundrechtsverletzungen billigend in Kauf. Selbst ein offenbar in der Anfangsphase schließlich vorhandener Filter für leitungsvermittelte Verkehre soll nur zu 95 Prozent funktioniert haben.[488] Das bedeutet bei Hundert erfassten Kommunikationen „rutschen“ im Durchschnitt fünf durch. Angesichts der potentiellen Masse erfasster Telekommunikation, sind dies nicht tolerierbare Grundrechtsverstöße.[489]

Für Internetverkehre (IP) ist die Filterung hochkompliziert. Anfangs- und Endpunkt einer Kommunikation lassen sich hierbei nicht bestimmen wie bei einer „normalen“ leitungsvermittelten Telefonverbindung. Dies war dem BND auch bekannt.

Der als erste Filterstufe für die Erfassung von IP-Verkehren vom BND entwickelte „Separator“ war jedoch schon vom Ansatz her unvollkommen. „Operationelle Schwachstellen“, die die „G 10-Konformität gefährden“ können, bescheinigte auch das BSI bei seiner „Zertifizierung“ im Oktober 2005.[490] Das mit dem Separator verfolgte Konzept, anhand von IP-Adressbereichen Kommunikation aus oder nach Deutschland erkennen zu wollen, kann immer nur grob sei. Eine erhebliche Unschärfe besteht aufgrund dynamischer IP-Adressen bzw. häufig zwischen TK-Anbietern wechselnden IP-Blöcken, die heute vielleicht Russland oder dem Iran, morgen jedoch wegen vielfacher Untervermietung von IP-Bereichen einem deutschen Provider zugeteilt sind. Auch weitere Filterstufen, die den Verkehr anhand der Top-Level-Domain .de bei E-Mails oder der deutschen Telefonvorwahl 0049 unterscheiden sollten, genügten einem umfassenden G 10-Schutz nicht. Weder eine E-Mail-Adresse noch eine Telefonnummer lassen

488) *Süddeutsche Zeitung* vom 4. Oktober 2014, „Codewort Eikonal“ „ http://www.sueddeutsche.de/politik/geheimdienste-codewort-eikonal-der-albtraum-der-bundesregierung-1.2157432..

489) Dass wir der Auffassung sind, dass Artikel 10 GG auch Ausländer_innen im Ausland schützt, soll hier zunächst unberücksichtigt bleiben; siehe dazu ausführlich in Kapitel V.3.b)bb) – Fernmeldegeheimnis als verfassungsrechtlicher Maßstab.

490) Siehe hierzu unter V.5 – EIKONAL: Unzulängliche BSI-Prüfung.

überhaupt hinreichenden Rückschluss auf die Nationalität der beteiligten Telekommunikationsteilnehmer_innen oder deren Aufenthaltsort zu.[491] Soweit nach dieser „Filterung“ fälschlicherweise Telekommunikationsverkehre von Deutschen oder mit Deutschandbezug als vermeintliche Auslandsverkehre qualifiziert wurden, sind diese unmittelbar in der weiteren Prozesskette der Operation EIKONAL unter Beteiligung der NSA verarbeitet worden. Fehler sollten in der Anfangsphase der Operation durch eine händische Prüfung durch BND-Mitarbeiter_innen bereinigt werden. Dies ist weder schlüssig noch angesichts der Datenmengen nachvollziehbar, schon gar nicht bei Verkehrsdaten oder Metadaten, die ohne den Einsatz von Selektoren oder Suchbegriffen stets komplett und daher massenhaft aus den ausgewählten Strecken erfasst wurden.

Daten aus leitungsvermittelter Kommunikation aus dem Frankfurter Netzknoten wurden nach Angaben von BND-Zeug_innen ab Frühjahr 2005 nur noch automatisiert gefiltert und ohne manuelle Nachkontrolle an die NSA übermittelt.[492] Für IP-Verkehre und insbesondere die daraus resultierenden Metadaten erscheint eine händische Prüfung aufgrund des Datenumfangs ausgeschlossen.

Es ging der NSA in der Kooperation – anders als uns die BND-Zeug_innen anfangs wiederholt weiß machen wollten – nicht um „Meldungen“, für die ein Nachrichtenbearbeiter des BND z. B. die Inhalte von E-Mails oder Telefonaten auf ihre Relevanz untersucht hat und daraus einen Bericht verfasst hat. Die NSA wollte von Anfang an die erfassten Rohdaten, also vollständige Kommunikationen und vor allem Metadaten aus dem Datenstrom am Kabelknoten.

d) BND-“Schwachstellenbericht“ bescheinigt Grundrechtsverstöße

Eine vom damaligen Leiter der Abteilung 2 im BND, *Urmann*, im Februar 2007 in Auftrag gegebene „Dokumentation“ über die technischen Systeme und Abläufe der Operation EIKONAL[493] kam zu einem vernichtenden Urteil im Hinblick auf den Schutz von

491) Siehe hierzu auch Kapitel V.7. – Ungelöste Filterproblematik.

492) Vgl. Feststellungsteil F IV.2.c)bb) – Wirkbetrieb Telefonie (2005 bis 2007).

493) Dokumentation GRANAT vom 2. August 2007 (sog. Schwachstellenbericht), MAT A BND-9/2 (Tgb.-Nr. 15/14 – STRENG GEHEIM, pauschal herabgestuft auf GEHEIM, nur zur Einsicht in der Geheimschutzstelle des Deutschen Bundestages), Anl. 01, Ordner 165, Bl. 37-175.

sog. G 10-Daten. Insgesamt deutlich mehr als ein Dutzend Schwachstellen im System und bei Prozessen identifizierte die Projektgruppe in ihrem Bericht von August 2007.

Da der Bericht weiterhin geheim eingestuft ist, können wir hier keine Details wiedergeben. Das darin festgestellte Ergebnis bewerten wir jedoch wie folgt: Der BND hat ein System eines anderen Nachrichtendienstes eingesetzt, bei dem er nicht wusste, was genau es macht und wie es konfiguriert ist. Der andere Dienst hatte allerdings Zugriff auf verschiedene Stellschrauben des Systems und konnte diese durch von ihm gelieferte Updates beliebig ändern, sodass die Durchschaubarkeit des Systems für den BND immer wieder aufgehoben wurde und nur mit unverhältnismäßigem Aufwand wiedererlangt werden konnte – bis zum nächsten Update.

Als Folge davon hatte die NSA Zugriff auf sog. G 10-geschütztes Material, also Kommunikationsdaten von Deutschen bzw. aus Deutschland. Der Bericht benennt dies im Übrigen an vielen Stellen nicht in der Möglichkeitsform, wie es BND-Zeug_innen und selbst die massiv eingeschüchterte Verfasserin des Schwachstellenberichts, die Zeugin *K. L.*, nachträglich vor dem Ausschuss behaupteten. Der Bericht spricht nicht von potentiellen G 10-Daten-Abflüssen, sondern von tatsächlichen.

Dass überhaupt G 10-geschützte Daten in die JSA gelangen konnten, verwundert. Angeblich sollten diese mit dem „Separator“ als Filter vorher ausgesondert werden. Sowohl im „Schwachstellenbericht“ als auch in dem zeitgleich beauftragten Bericht zum „Separator“ werden dann exakt die Probleme, die schon die BSI-Prüfung zwei Jahre zuvor im Herbst 2005 aufgeworfen hatte, virulent: Nicht aktuelle IP-Adressbereichslisten und – viel gravierender – das konzeptionelle Versagen des Systems, über IP-Adressen „geschützte“ TK-Teilnehmer_innen erkennen zu wollen. Dem BND war im Frühjahr 2007, als er bereits tief in der Erfassung von IP-Verkehren aktiv war, absolut klar, dass das bestehende Filtersystem ungenügend war.

Der NSA mussten in der Kooperation bei EIKONAL auch keine Daten in dem Sinne „übermittelt“ werden. In der JSA in Bad Aibling, dort wo die Daten aus dem Kabelabgriff aufliefen, arbeiteten BND und NSA zusammen – mit einem gemeinsamen Zugriff auf die Daten, bis mindestens Herbst 2007 sogar in einem gemeinsamen Netzwerk. Alles, was in das gemeinsame System floss, stand der NSA zur Verfügung.

Wir gehen daher davon aus, dass der BND der NSA bei der Operation EIKONAL auch massenhaft Telekommunikationsdaten von Deutschen bzw. mit Deutschlandbezug rechtswidrig zugänglich gemacht hat.

Angesichts des verheerenden Ergebnisses des Schwachstellenberichts hätte der BND die Operation EIKONAL umgehend, d. h. spätestens im Sommer 2007 abbrechen müssen. Den Bericht oder wenigstens dessen Befunde hat der damalige Abteilungsleiter 2 nach eigenem Bekunden weder dem Präsidenten noch dem Kanzleramt zur Kenntnis gegeben. Bei solcherart gravierender Grundrechtsverstöße (selbst wenn sie nur potentielle gewesen wären) und einer derart für den BND bedeutsamen Kooperation mit der NSA hätte dies zwingend gemeldet müssen, um eine Entscheidung der Vorgesetzten zu erwirken.

Stattdessen wurde – wenn auch möglicherweise mit einer kurzen Unterbrechung – weitergemacht. Der damalige Projektleiter von EIKONAL, der Zeuge *S. L.* bestätigte einen sog. „Wirkbetrieb“ für IP-Verkehre ab Mitte/Ende 2007 bis Juni 2008 mit Weiterleitung der Daten an die JSA.[494] Schlechterdings unvorstellbar ist, dass der BND die im Schwachstellenbericht benannten gravierenden Probleme und Defizite – wie BND-Zeug_innen behaupteten – in dieser kurzen Zeit behoben haben soll. Vollends unglaubwürdig wird die vom BND (und der Koalition) kolportierte Geschichte dadurch, dass der Wirkbetrieb nach neun Monaten im Sommer 2008 komplett eingestellt und die Operation EIKONAL damit beendet worden sein soll. Als Grund wurde sogar gegenüber dem Kanzleramt angeführt, dass der G 10-Filter nicht funktionierte und auch auf absehbare Zeit nicht funktioneren würde:

> „Das Vorhaben scheiterte daran, dass es technisch nicht möglich ist, eine absolute und fehlerfreie Trennung von geschützter und ungeschützter Kommunikation zu erreichen.“[495]

---

494) *S. L.*, Protokoll-Nr. 26 I, S. 66.; siehe hierzu auch im Feststellungsteil unter F.IV.4.c) – Wirkbetrieb IP (Ende 2007 bis Juni 2008)

495) Zitiert nach *Süddeutsche Zeitung* vom 4. Oktober 2014, „Codewort Eikonal“ „ http://www.sueddeutsche.de/politik/geheimdienste-codewort-eikonal-der-albtraum-der-bundesregierung-1.2157432..

Die Probleme aus dem Schwachstellenbericht waren offenkundig nicht behoben.

Der versagende G 10-Filter war sicherlich ein Grund für das (zu späte) Ende der Operation. Aufgrund der Unterlagen kommen wir zu dem begründeten Schluss, dass EIKONAL auch wegen des Verdachts abgebrochen wurde, die NSA würde Aufklärung gegen Deutschland und Staaten der EU betreiben. Ebenso die späteren, in den Medien wiedergegebenen Warnungen des BND an das Kanzleramt und dessen damaligen Chef *de Maiziére* aus den Jahren 2008 bis 2010[496] weisen in diese Richtung.

Der BND zog die Notbremse, weil er die US-Technik und die NSA nicht im Griff hatte – und sich der US-amerikanische Geheimdienst nicht an die Regeln halten wollte.

e) Versagen der Fachaufsicht in BND und Kanzleramt

Dass es im Rahmen der Operation EIKONAL zu Rechtsverstößen und Grundrechtsverletzungen durch Verletzung des Fernmeldegeheimnisses aus Artikel 10 GG kommen konnte, ist sowohl der BND-Spitze als auch dem Aufsicht führenden Kanzleramt anzulasten.

Begünstigt wurden die Verstöße durch die Konstruktion der JSA als US-deutsche Arbeitseinheit und durch das System der BND-Außenstellen generell. Diese konnten von der Zentrale relativ unkontrolliert arbeiten. Das genannte Problem der „Amerikanisierung“ der BND-Mitarbeiter_innen in der JSA, dass durch die tägliche Zusammenarbeit mit den NSA-Kolleg_innen entstanden sein mag, sowie der Druck, die Kooperation zum Erfolg zu führen, können derart schwere Verstöße keinesfalls entschuldigen, allenfalls zum Teil erklären.

Verantwortlich war im BND zu allererst die eigene Fach- und Dienstaufsicht durch den Abteilungsleiter und den Präsidenten – im fraglichen Zeitraum waren dies *Hanning* und *Uhrlau*.

Ein Eingreifen des Kanzleramtes konnte nicht festgestellt werden. Dessen Fachaufsicht über den BND bei der Operation EIKONAL bestand im Wesentlichen darin, dem

496) Bspw. *Frontal21* vom 27. April 2015, „Nachgehakt – US-Wirtschaftsspionage: de Maiziere war ab Februar 2008 informiert“, vgl. https://www.zdf.de/ZDF/zdfportal/blob/38338402/1/data.pdf.

BND diese Kooperation mit der NSA zu ermöglichen (beginnend mit dem „Freibrief" an die *Telekom*, der Befürwortung einer G 10-Anordnung zum Schein etc.). Selbst als dem damaligen Chef des Kanzleramtes *de Maizière* und dem Abteilungsleiter 6, *Fritsche*, Ende 2007/Anfang 2008 vom BND Probleme mit der NSA bei der Operation EIKONAL und den G 10-Filtern vorgetragen wurden, stoppte offenbar keiner von ihnen die Operation.

f) BND als Teil des NSA-Programms RAMPART-A

Die Einrichtung eines Kooperationsprojekts vergleichbar der JSA und auch die gesamte Systematik eines gemeinsamen Erfassungs- und Verarbeitungsprozesses wie bei der Operation EIKONAL wird von der NSA selbst in mehreren Vortragsunterlagen aus den Jahren ab 2010 beschrieben, die der Ausschuss aus den veröffentlichten *Snowden*-Dokumenten beigezogen hat. So beschreibt die NSA das schon 1992 in Gang gesetzte „RAMPART-A"-Programm mit „Drittpartnern", zu denen generell auch Deutschland zählt, wie folgt:

> „Deckname für das unkonventionelle Special-Access-Programm (für besonderen) Zugang der NSA.
>
> – Für Zugriff auf internationale Glasfaserkabel mit hoher Kapazität, die die weltweit wichtigsten Congestion Points [Datenstau-Punkt im Internet] kreuzen."[497]

Und weiter:

> „Ausgehandelte Rahmenvereinbarungen:
>
> – Ausländische Partner bieten Zugang zu Kabeln und nutzen US-Geräte

497) MAT A Sek-6c_DE, Bl. 3; Übersetzung durch den Sprachendienst des Deutschen Bundestages; abrufbar unter https://edwardsnowden.com/wp-content/uploads/2014/06/tssinframpartaoverview-v1-0-redacted-information.pdf [abgerufen am: 15. Juni 2017].

> – USA stellen Geräte für [Daten-]Transport, Verarbeitung und Analyse
>
> – Keine Erhebung von US-Daten seitens des Partners, keine Erhebung von Daten aus dem Gastgeberland seitens der USA
>
> – Gemeinsame Aufgabenzuweisung und Datensammlung.“[498]
>
> „Deckung
>
> Die meisten Drittpartner von RAMPART-A arbeiten im Schutz von öffentlich bekannten Comsat-Maßnahmen [Kommunikationssatelliten] an Glasfaserprojekten“[499]

Weiter heißt es explizit:

> „Das RAMPART-A-Programm liefert durch spezielle Zugriffsinitiativen in weltweiten SIGINT-Partnerschaften Erhebungen von Langstreckenkommunikation aus internationalen Mietleitungen. (…) RAMPART-A hat im Umfang von über 3 Terrabyte pro Sekunde Zugriff auf weltweit strömende Daten, dies schließt sämtliche Kommunikationstechnologien ein, darunter Stimmanrufe, Fax, Telex, E-Mail, Internet-Chat, Virtual Private Network (VPN, Virtuelle private Netze), Voice over IP (VoIP, Internettelefonie) und Anrufaufzeichnungen.“[500]

Hinsichtlich der erwähnten Rahmenvereinbarung, gegenseitig auf die Erhebung von Daten der beteiligten Partner bzw. der USA zu verzichten, wird an anderer Stelle klargestellt, dass dabei auch „Ausnahmen möglich“ seien.[501] Welche das sein können, aus

498) MAT A Sek-6c_DE, Bl. 3.

499) MAT A Sek-6c_DE, Bl. 10.

500) MAT A Sek-6b_DE, Bl. 1, abrufbar unter https://edwardsnowden.com/wp-content/uploads/2014/06/foreignpartneraccessbudgetfy2013-redacted.pdf [abgerufen am: 15. Juni 2017].

501) MAT A Sek-6d_DE, Bl. 6, abrufbar unter https://edwardsnowden.com/wp-content/uploads/2013/11/sso4.pdf [abgerufen am: 15. Juni 2017].

welchen Gründen und dass der beteiligte Partner darüber informiert sei, wird nicht mitgeteilt. Ohnehin würden Partner nie über den Hintergrund der verwendeten Suchbegriffe und Selektoren informiert. So heißt es über die von der NSA zur Erfassung verwendeten „Targets“ (Ziele) ausdrücklich:

> „Zugänglich sind lediglich die Zieldeskriptoren, keine Kommentare/Erweiterung“[502]

Dies beschreibt exakt jenen Rahmen, der auch von den Zeug_innen des BND für die Kooperation mit der NSA beschrieben wurde und den die beigezogenen Materialien und Akten abbilden. Es lässt den Schluss zu, dass EIKONAL eine Operation im Rahmen von RAMPART-A war und der BND ein Partner der NSA bei dessen weltweiter Massenüberwachung ist.

In den Präsentationsfolien zu RAMPART-A finden sich mehrmals Schaubilder,[503] die eine „typische RAMPART-A-Operation“ abbilden und die Wege der Datenweiterleitungen zeigen sollen. Darin fällt zum einen auf, dass die Bezeichnungen für den „Abgriffspunkt“ („Site A“), das „Verarbeitungszentrum“ („Site B“) sowie für die „Analysten des Partners“ („Site C“) exakt den vom BND im Schwachstellenbericht verwendeten entsprechen. Ein Zufall erscheint äußerst unwahrscheinlich. Zum anderen ist bemerkenswert, dass es in den Folien eine direkte Verbindung mittels Kabel oder Satellit über ein „COMINT NETWORK“ zwischen dem Verarbeitungszentrum („Site B“), was im Fall von EIKONAL der Betriebsraum bei der Telekom in Frankfurt ist, und der NSA gibt. Die BND-Zeug_innen haben erwartungsgemäß ausgeschlossen, dass eine (heimliche) Ausleitung von Daten aus dem Abgriff in Frankfurt durch die NSA stattfindet. Der damalige Abteilungsleiter 2, *Breitfelder*, ging allerdings ganz allgemein – wie eingangs zitiert – „davon aus, dass die das machen.“

Der BND hat sich ersichtlich in eine Struktur einbinden lassen, die er weder überschaute noch kontrollieren konnte. Der Wunsch, auf Augenhöhe im internationalen

---

502) MAT A Sek-6e_DE, Bl. 1, abrufbar unter https://edwardsnowden.com/wp-content/uploads/2014/06/uodds2overview-v1-1-redacted-information-dk.pdf [abgerufen am: 15. Juni 2017].

503) MAT A Sek-6c_DE, Bl. 9; MAT A Sek-6d_DE, Bl. 8.

Konzert der Technischen Nachrichtendienste agieren zu können, sollte mit dem Tauschhandel Daten gegen Technik auf möglichst kurzem Wege verwirklicht werden. Selbst die wie in einer der RAMPART-A-Folien genannten fehlenden Erläuterungen bei den gelieferten NSA-Selektoren, sollten im Verlauf der Kooperation dem BND auf die Füße fallen.[504]

7. Ungelöste Filterproblematik

a) DAFIS: Filterung misslungen

Der BND gab an, dass die an die NSA übermittelten Inhaltsdaten lediglich auf vorher festgelegten Satellitenstrecken erfasst würden und nach deutschen und europäischen Interessen sowie nach „G-10“-Gesichtspunkten – zumindest jenen die der BND dafü hielt – „gefiltert“ würden.[505] Das hier in Rede stehende Datenfilterungssystem (DAFIS), ist äußerst mangelhaft.[506] Das Filtersystem wurde zum einen eingesetzt, die von der NSA bereit gestellten Telekommunikationsmerkmale (Selektoren) zu überprüfen. So sollte sichergestellt werden, dass sich die „Auftragserfassung“ nicht gegen deutsche und europäische Ziele und Interessen richtet.

Bis 2006 versuchten die BND-Mitarbeiter_innen in Bad Aibling noch die Selektoren manuell zu überprüfen. Da dies vor allem aufgrund der schieren Massen nicht funktionierte und als der BND feststellte, dass die NSA explizit nach Informationen suchte, die nach einer solchen Prüfung nicht mehr übermittelbar wären, behilf sich der BND mit der Herstellung eines entsprechenden Systems, das bei der Lösung des Problems helfen sollte. Tatsächlich stellt es selbst eines dar. Das wusste auch der BND, weshalb er sich zwar öffentlich darauf berief, intern jedoch damit beschäftigt war, die *DAFIS* zum Laufen zu bringen. Entwicklung zog sich über Jahre hin und ist bis heute nicht vollumfänglich abgeschlossen.

---

504) Siehe Kapitel V.8 – Verstöße bei der Verwendung von NSA-Selektoren.

505) Ergebnisprotokoll, Vorbesprechung des Kontrollbesuchs des BfDI in Bad Aibling am 2. und 3. Dezember 2013, MAT A BK-1/6b, Bl. 434 (VS-NfD).

506) *G.L.*, Protokoll-Nr. 24 II – Auszug offen, S. 94.

Zeuge *Reinhardt Breitfelder*: „Wir hatten eine Furcht. Wir hatten die Furcht, dass, ohne dass wir es merken, G-10-Material irgendwie abfließt, dass wir das nicht im Griff haben technisch; deswegen ja auch die Prozessunterbrechungen oft mit händischen Prüfungen. Das war der Kern unseres rechtlichen Problems. Dass wir zugreifen durften, das stand im BND-Gesetz. Mit der G-10-Anordnung war das noch mal abgesichert. Da hatten wir keine Probleme. Die Probleme waren nur, dass wir im Eingriff selber Fehler machen oder Abflüsse nicht merken, die durch die Technik geschehen. Deswegen haben wir ja auch eher etwas weggesteuert, gegen Erde geleitet, vernichtet, als dass wir es weitergegeben haben."

Hans-Christian Ströbele (BÜNDNIS 90/DIE GRÜNEN): „Kann man das so zusammenfassen, dass diese rechtlichen Bedenken darin bestanden, dass Sie nicht sicher sein können, technisch jetzt nicht sicher sein können, dass Sie tatsächlich alle G-10-Sachen ausfiltern?"

Zeuge Reinhardt Breitfelder: „Ja".[507]

Die drei „Filterstufen" wurden jedes Mal weiterentwickelt, wenn der BND merkte, die „Filterung" ist unzureichend. Tatsächlich handelt es sich hierbei auch größtenteils um Listen, in denen die Daten – ohne Vorgaben zur Aufnahme – geführt werden, die der BND als „verboten" angesehen hat.[508] Diese Daten wurden mit dem Datenstrom angeglichen und bei einem Treffer ausgefiltert, alle anderen blieben im Datenstrom und wurden weitergeleitet.

Dazu gehörte eine Positivliste mit u.a. deutschen Unternehmen, Organisationen usw, die immer wieder ausgesondert werden sollten für den Fall, dass Daten die. So sollte verhindert werden, dass eigentlich schon unzulässig erhobene daten im Prozess in der entsprechenden Verarbeitungsstufe wieder ausgesondert werden sollten. Bis kurz

507) *Breitfelder* und *Ströbele*, MdB Die Grünen/Bündnis90, Protokoll-Nr. 28 I, S. 61.

508) Schindler, Protokoll-Nr. 50 I, S. 75.

vor den Enthüllungen *Edward Snowdens* enthielt diese Positivliste rund 500(!) Einträge. Diese Anzahl hat sich seitdem stark erhöht. Das bestätigt, dass die Filterung – konkret die Ausfilterung von geschützten deutschen Unternehmen, Bürger_innen und Organisationen unvollständig war. Die vom Zeugen Breitfelder geschilderte Angst war berechtigt. Die Bedenken gegen die – erkanntermaßen – rechtswidrige, weil unzulängliche Praxis hatten aber keine Auswirkungen auf die jahrelange Praxis.

b) Filterung technisch nicht möglich

Eine zuverlässige Filterung inländischer und ausländischer Verkehre ist schon technisch gar nicht zu erreichen. Zur Möglichkeit der Unterscheidung dieser Datenverkehre insbesondere in Hinsicht auf technische Möglichkeiten, ob eine Datenerfassung deutscher Grundrechtsträger_innen ausgeschlossen werden kann, hat der Ausschuss zwei Sachverständigengutachten erstellen lassen. Im Gutachten von *Kay Rechthien* heißt es dazu gleichermaßen einleitend wie zusammenfassend:

> „Eine einfache Unterscheidung zwischen inländischem und ausländischem Datenverkehr ist durch die Komplexität der Netzstruktur, die Vielfalt der Dienstemodelle – Stichwort Cloud-Services – und die schnellen Veränderungen von Routing-Pfaden, Netzbelegungen, die enormen Bandbreiten und die vielfache Schachtelung der Datenverkehre auf den Glasfaserleitungen nicht mehr möglich.“[509]

Das Sachverständigengutachten von *Gabi Dreo Rodosek* kommt zu ähnlichen Resultaten und nicht, wie im Feststellungsteil fälschlich konstatiert, „zu unterschiedlichen Ergebnissen“.[510]

Der Zeuge *Klaus Landefeld* sagte aus, dass das Filtersystem des BND Ergebnisse mit einer Genauigkeit von weniger als 100 Prozent liefert und führte hypothetisch am Bei-

509) Sachverständigengutachten von *Rechthien*, MAT A SV-13/3, Bl. 2.

510) Feststellungen des Untersuchungsausschusses, Kap. F. I. 4. b) bb) aaa).

spiel des *DE-CIX* Knotenpunkts aus, dass ein dortiger Abgriff mit diesem System immernoch „mehrere Millionen fehlerhaft bewerteter Verbindungen jeden Tag bedeuten“[511] würde.

aa) Stellungnahme des Sachverständigen *Rechthien*

Auf aktuell installierten Leitungen, so ist *Rechthiens* Gutachten zu entnehmen,[512] kann pro Faserpaar eine Datenmenge von 19,2 TBit/s (19200 GBit/S) transportiert werden, wobei die Anzahl der in einer Leitung gebündelten Faserpaare differiert: von 4 bis 12 in Unterseekabeln bis zu mehreren Hundert beispielsweise in städtisch verlegten Glasfaserkabeln. Sollen bestimmte Netz-Verbindungen gezielt ausgeleitet werden, ist dazu die Analyse tieferer Protokollschichten mittels Deep Packet Inspection (DPI) prinzipiell in der Lage. Doch ist das Verfahren sehr aufwendig, kostenintensiv und aufgrund technischer Kapazitätsbegrenzungen ineffizient:

> „Heute verfügbare Hardware für die tiefere Analyse ist in der Regel für Bandbreiten von 100 Gbit pro Schnittstelle ausgelegt, also etwa einem Zweihundertstel der auf einem Faserpaar transportierbaren Bandbreite. Um eine 19,2-Tbit/s-Faser vollständig zu überwachen, müssten etwa zweihundert dieser Systeme installiert werden.“[513]

Effizienter in der Überwachung des Datenverkehrs sind *Rechthien* zufolge statistische Verfahren auf Basis von Samplingtechniken. Dazu wird ein Bruchteil, nach dem standardisierten Analyseverfahren sFlow jedes 16000ste Paket, des Datenverkehrs ausgeleitet sowie Absender-, Zieladresse und (anwendungsspezifisches) Internet-Protokoll anhand des Headers eines Datenpakets ausgelesen. Doch lassen sich mit solchen

---

511) Praktische Auswirkungen und technische Implikationen des Entwurfs eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes (Bundestagsdrucksache 18/9041), Berlin, 14. Oktober 2016, S. 7. Abrufbar unter: https://www.eco.de/wp-content/blogs.dir/20161014-_eco_stn_-bndg-e.pdf.

512) Sachverständigengutachten von *Rechthien*, MAT A SV-13/3, passim.

513) Sachverständigengutachten von *Rechthien*, MAT A SV-13/3, Bl. 12.

Verfahren immer nur Analysen über „einen groben Durchschnitt der Arten des Verkehrs“[514] gewinnen. Statistische Auswertungen auf Grundlage von Sampling, aber auch auf Basis von (partiellem, stichprobenartigem) DPI bieten entsprechend kaum Möglichkeiten, „globale Aussagen über die Zusammensetzung des Internetverkehrs zu machen.“[515] Zwar wird auf deren Basis erkennbar, welche Applikationen genutzt werden und wieviel Verkehr fließt, doch ist die Zusammensetzung der Verkehre neben Uhrzeit, Netzwerkanbieter und Punkt des Datenabgriffs insbesondere davon abhängig, welche Daten von Kund_innen jeweils auf einer Verbindung gebündelt transportiert und üblicherweise in einer von Dritten angemieteten Transportkapazität terminiert werden.

Tenor des Sachverständigengutachtens *Rechthiens* ist an dieser Stelle, dass im Falle von paketvermittelter Kommunikation nationale (Inland-Inland), internationale (Inland-Ausland) und transnationale (Ausland-Ausland) Verkehre gezielt weder streckenbezogen auf konkret benannten Übertragungungswegen ausfindig zu machen sind noch sich streckenbezogen auf solchen voneinander separieren lassen. Ferner werden Methoden und Grenzen gängiger IP-Geolokalisationstechniken zur Ermittlung der geographischen Position einer Quell- oder Zieladresse beschrieben und analysiert.[516] Eine Triangulierung auf Latenzbasis ist demnach unter Laborbedingungen mit detaillierter Genauigkeit möglich, in Echtzeit aber durch äußere Einflüsse sehr anfällig, sodass es beispielsweise bei hoher Verkehrslast in Weitverkehrsnetzen zu geographischen Abweichungen in der Ortsbestimmung kommt, deren Bestimmungsungenauigkeit mehrere hundert Kilometer betragen kann. IP-Geolokalisationstechniken hingegen, die auf Einträge in der Routingstabelle, Registrierungsdatenbanken und Traceroutes (Ermittlung der Verbindungspfade) zugreifen, sind abhängig von der Aktualität und Transparenz der vorgehaltenen Informationen. Das es dabei schnell zu Zugriffen auf irreführende Einträge kommen kann, wird anhand des Tausches von IP-Adress-Blöcken ei-

514) Sachverständigengutachten von *Rechthien*, MAT A SV-13/3, Bl. 9.

515) Sachverständigengutachten von *Rechthien*, MAT A SV-13/3, Bl. 10.

516) Sachverständigengutachten von *Rechthien*, MAT A SV-13/3, Bl. 13-14.

nes multinationalen Konzerns mit Tochterunternehmen in mehreren Ländern exemplifiziert. Ferner bestehen für alle Verfahren der Geolokalisation Funktionalitätsgrenzen im Falle von nicht öffentlich erreichbaren IP-Netzwerken, nicht aussagefähigen Hostnamen sowie implementierten Filtern oder Verkehrsleitung mittels Multiprotocol Label Switching (MPLS). In der Synopse zur IP-Geolokalisation heißt es bei *Rechthien* daher:

> „Keine der Methoden ist aber genau genug, um sicher festzustellen, wo sich eine IP-Adresse wirklich befindet."[517]

bb) Stellungnahme der Sachverständigen *Dreo Rodoseck*

Auch *Dreo Rodoseck* charakterisiert die gängigen Verfahren zur Differenzierung und Quantifizierung des Datenverkehrs analog zu *Rechthien*. DPI, so heißt es, biete methodisch zwar „den besten Einblick in den Netzverkehr", unterliege aber einer „Big Data Problematik", „da es praktisch kaum machbar ist, die Gesamtheit der Daten aufzuzeichnen und zu verarbeiten."[518] Grund dafür sei, dass sehr große Speicher- und Rechenkapazitäten benötigt würden, um die Menge an Daten mit der notwendigen Verarbeitungsgeschwindigkeit zu bearbeiten. Zudem werde die Datenauswertung beispielsweise durch Paketfragmentierung und asymmetrisches Routing erschwert. Vorteil des Industriestandards sFlow hingegen sei „die geringe Datenmenge, die gespeichert, verarbeitet und analysiert werden muss", dem als Nachteil „die geringere Genauigkeit der Klassifizierung im Vergleich zu DPI" gegenüberstehe.[519] Zusätzlich, darin in Ergänzung zu *Rechthien*, benennt *Dreo Rodosek* den sogenannten Port-basierten Ansatz, der „aber nicht zwangsläufig zuverlässige Ergebnisse" liefere, dennoch „für eine erste Klassifizierung geeignet" sei.[520] „Letztendlich", so lautet ihr Fazit, sei auf der

517) Sachverständigengutachten von *Rechthien*, MAT A SV-13/3, Bl. 13.

518) Sachverständigengutachten von *Dreo Rodosek*, MAT A SV-13/2, Bl. 13.

519) Sachverständigengutachten von *Dreo Rodosek*, MAT A SV-13/2, Bl. 14.

520) Sachverständigengutachten von *Dreo Rodosek*, MAT A SV-13/2, Bl. 13.

Grundlage aller drei genannten Verfahren „eine vollständige Differenzierung des Datenverkehrs in der Regel nicht möglich.“[521]

Gleichartig fallen im Sachverständigengutachten *Dreo Rodosek* ebenfalls die Aussagen zu Übertragungsstrecken aus. Demnach sind diese einerseits „i.A. nicht für den Ausland-Ausland-Telekommunikationsverkehr dediziert“, kann dementsprechend jede gewählte Übertragungsstrecke auch Inland-Ausland- und Inland-Inland-Verkehre enthalten, und andererseits „nicht statisch“, sodass sich der Anteil der Ausland-Ausland, Inland-Ausland- und Inland-Inland-Verkehre auf einer ausgewählten Übertragungsstrecke jederzeit ändern kann.[522] Kongruent sind ebenso entsprechende Feststellungen zur Bewertung gängiger Verfahren der IP-Geolokalisation. *Dreo Rodosek* unterscheidet aktive und passive Methoden. Erstere basieren auf aktiven Messungen zur Korrelation zwischen Latenzwerten und geographischen Distanzen. Letztere stützen sich auf Verfahren zur Extraktion standortbezogener Informationen zu einer gegebenen Adresse unter Zugriff auf umfangreiche Datenbestände, wie sie beispielsweise aus Abfragen von Registrar-Adressbereichen, topologischen Verbindungspfadauflösungen oder Geoservice-Anbietern zu gewinnen sind. Nur passive Methoden können demnach im Rahmen von großen Datenmengen „als nutzbar erachtet werden“, während aktive Messungen zwar „grundsätzlich genauer, allerdings auch ressourcenintensiver und daher nur für einzelne IP-Adressen in Erwägung zu ziehen“ sind.[523] Zusammenfassend stellt *Dreo Rodosek* fest:

> „Eine Identifikation der Ursprungs- und Zielorte der Kommunikationsvorgänge kann in der Regel nur grob granular und bei nicht eingesetzten Verschleierungsmaßnahmen erfolgen. Auf Grundlage von Verfahren wie IP-Geolokalisation können hinreichend zuverlässige Entscheidungen getroffen werden, ob sich die Quell- oder Ziel-IP-Adresse eines Datenpakets im Ausland befindet.“[524]

521) Sachverständigengutachten von *Dreo Rodosek*, MAT A SV-13/2, Bl. 14.

522) Sachverständigengutachten von *Dreo Rodosek*, MAT A SV-13/2, Bl. 21.

523) Sachverständigengutachten von *Dreo Rodosek*, MAT A SV-13/2, Bl. 28.

524) Sachverständigengutachten von *Dreo Rodosek*, MAT A SV-13/2, Bl. 34.

Die Charakterisierung „hinreichend zuverlässige Entscheidungen“ allerdings wird von *Dreo Rodosek* im Weiteren nicht näher ausgeführt, geschweige denn in Hinsicht auf eine Grundrechtsrelevanz in der Erfassung der Komplementärmenge oder des nicht hinreichenden Rests quantifiziert. Zur Genauigkeit von aktiven und passiven IP-Geolokalisationstechniken mit Fokus auf Europa hält *Dreo Rodosek* demgegenüber fest, dass die durchschnittlichen Abweichungen in der Ortsbestimmung dieser Verfahren zwischen 134 und 770 Kilometern betragen. Die quantitavie Genauigkeit „zur Lokalisation einer IP-Adresse auf Landesebene“ auf Basis des Zugriffs auf Geodatenbanken wird zudem unter Zugrundelegung entsprechender Forschungsliteratur „mit 96% bis 98%“ benannt.[525]

cc) Angaben des Zeugen *Klaus Landefeld*

Aus der Praxis werden die Ergebnisse der Gutachten, dass eine Trennung von deutschen und nicht-deutschen IP-Verkehren ebenso wenig möglich ist wie eine Ausfilterung zu 100 Prozent, bestätigt. Der Zeuge *Landefeld*, Beirat der *DE-CIX Management GmbH* und Vorstandmitglied des *Verbands der Internetwirtschaft eco*, hat in seiner Vernehmung zur geographischen Zuordnung auf Basis von Datenbanken ausgeführt:

> „Also, gerade wenn es um IP-Adressen geht, ist das zwar mit einer gewissen Qualität möglich, aber eben nicht 100 Prozent. Es gibt dafür Datenbanken. Also das, was Sie aus den Registries ziehen können, das funktioniert, na ja, mehr schlecht als recht, weil das eben die Frage ist: Was wird einer Organisation zugewiesen? – Aber da passiert zum Beispiel – – Also in Europa ist die Vergabe typischerweise durch RIPE. Das ist die Organisation, die das Ganze vergibt, aus Amsterdam.
>
> Und wenn ich dort als Provider – gerade als paneuropäischer Provider – einen Blog beantragt habe in der Vergangenheit, dann wurde der mir zugeteilt und war im Zweifelsfall zur Vergabe in ganz Europa. Also,

525) Sachverständigengutachten von *Dreo Rodosek*, MAT A SV-13/2, Bl. 29.

> diese Frage „Wo ist das? Wo ist das genau zugeteilt? Wohin läuft das?“ ist nicht trennscharf zu beantworten.
>
> Es gibt allerdings wieder Unternehmen, die es sich zur Aufgabe gemacht haben, das zu tun. Das wird zum Beispiel sehr gerne eingesetzt bei der Zuordnung in elektronischen Shopping-Systemen oder bei diesen Blogging-Listen, wenn Sie Media Content abrufen wollen oder so was. Diese Datenbanken gibt es. Die sind auch teilweise – manche – bis auf Straßenblöcke genau oder so was Ähnliches. Aber auch die sind weder vollständig. Das funktioniert sozusagen andersrum. Dort gib es Positivinformationen, wo man sagen kann, diese IP-Adresse gehört da und da hin, wenn Provider das melden, weil es für diese Zwecke sinnvoll ist. Allerdings sind die eben, wie gesagt, weder vollständig noch sehr genau für die Adressen von den Providern, die nicht teilnehmen. Von daher sind diese IP-Datenbanken immer – – Also, es ist eine interessante Frage, wie viel Prozent Genauigkeit sie erreichen. Das läuft halt gegen die Frage: Wie viele Fehler wären akzeptabel? Wenn überhaupt.“[526]

Und zur grundsätzlichen technischen Möglichkeit einer G 10-Filterung erklärte er:

> „Wie gesagt, das ist eine Frage, wie gut Ihr Filter ist. Also wenn Sie jetzt 99 Prozent der IP-Adressen richtig haben oder 99,5 Prozent der IP-Adressen richtig haben – – Sie werden nie eine Datenbank bekommen, wo 100 Prozent der IP-Adressen richtig sind. Das ist allein dadurch, wie das angelegt ist, nicht da. Also ist die Frage – – Ist eigentlich nur noch eine Frage: Wie gut ist die Qualität? – Aber absolut wird sie nicht sein.“[527]

Die Frage nach der Qualität der G 10-Filter von IP-Verkehren schließt die Frage ein, in welcher Quantität deutsche Grundrechtsträger_innen von der Datenerfassung nicht

526) *Landefeld*, Protokoll-Nr. 43 I, S. 70 f.

527) *Landefeld*, Protokoll-Nr. 43 I, S. 73.

ausgeschlossen werden können. Abweichungen unter 100 Prozent in Geolokalisationsfiltern zeitigen allein aufgrund der Größenordnung der Verbindungszahlen im IP-Bereich quantitative Auswirkungen mit Grundrechtsrelevanz von enormen Ausmaßen. Das macht ein Rechenbeispiel anhand des in puncto Datendurchsatz weltweit größten Internetknotens *DE-CIX* in einer Stellungnahme des *eco* deutlich:

> „Die besten derzeit auf dem Markt erhältlichen, kommerziellen Filtersysteme zur Separierung von IP-Verkehren mit Regionalbezug erreichen derzeit Filterqualitäten von ca. 99,5 %. Das im NSA-Untersuchungsausschuss beschriebene, durch den Bundesnachrichtendienst selbst entwickelte System, welches für die Filterung der G 10 Verkehre verwendet wird, dürfte nur eine Genauigkeit von ca. 95-96 % erreichen.
>
> Hierbei ist zu berücksichtigen, dass die Verbindungszahlen im IP-Bereich sehr viel höher sind als bei klassischer Kommunikation. So werden beispielsweise am Netzknoten DE-CIX jeden Tag mehrere Milliarden Verbindungen verarbeitet. Legt man eine Genauigkeit bei der Filterung von 99.5% zugrunde (was mit dem beschriebenen System nicht möglich sein dürfte) oder ginge von einer unrealistischen Genauigkeit der IP-Filterung von 99.9% aus, würde dies am Beispiel des Datenknoten DE-CIX mehrere Millionen fehlerhaft bewerteter Verbindungen jeden Tag bedeuten.“[528]

Der vom BND gewählte und vom BSI fehlerhaft gebilligte Ansatz, dass Telekommunikationsverkehrsdaten auf Basis einer Geolokalisation geografisch zugeordnet und so gefiltert werden könnten, sehr ungenau und fehlerbehaftet ist. Die Beschreibung der angeblich mehr als 90%-igen Filtergenauigkeit ersetzt und genügt nicht den gesetzlichen Schranken. Sie soll vielmehr davon ablenken, dass schon wenige Prozent oder

528) Praktische Auswirkungen und technische Implikationen des Entwurfs eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes (Bundestagsdrucksache 18/9041), Berlin, 14. Oktober 2016, S. 7. Abrufbar unter: https://www.eco.de/wp-content/blogs.dir/20161014-_eco_stn_-bndg-e.pdf.

Prozentpunkte fehlerhaft zugeordneter Daten die rechtswidrige Überwachung einer unüberschaubaren Zahl Betroffener bedeutet. Rechtsverletzungen werden aber nicht geheilt, weil sie sich in einem vermeintlich geringen Prozentbereich bewegen.

8. Verstöße bei der Verwendung von NSA-Selektoren

Die NSA hat dem BND Suchbegriffe für die gemeinsame Erfassung im Rahmen der Operation EIKONAL sowie für die Satellitenüberwachung in Bad Aibling übermittelt. Suchbegriffe – auch Selektoren genannt – können Telefonnummern (Festnetz/Mobil), E-Mail-Adressen, SIM-Kartennummern (IMSI) und Gerätekennungen bei Handys (IMEI), *Facebook*- und Messenger-IDs, IP-Adressen, Webseiten-Adressen, aber auch Begriffe oder Namen u. v. a. mehr sein.

Solche Selektoren hat der BND in seinen Datenerfassungssystemen eingesetzt, um damit überwachte Telekommunikationsströme aus Glasfaserkabeln und Satelliten-kommunikation zu durchsuchen.

Zu Beginn der Operation EIKONAL im Jahr 2005 waren es mehrere hunderttausend Suchbegriffe der NSA – überwiegend Telefonnummern (und E-Mail-Adressen). Im Jahr 2015 lag die Anzahl nach Medienberichten bei über 14 Millionen NSA-Selektoren,[529] die im Laufe der Kooperation an den BND übermittelt worden waren.

a) Ungenügende Prüfung der NSA-Selektoren durch den BND

Bereits das gesamte Konzept, quasi im Auftrag der NSA mit deren Suchbegriffen Telekommunikation zu erfassen, an der der BND selbst gar nicht zwingend interessiert ist, ist rechtlich fragwürdig (dazu unten mehr). Rechtswidrig ist diese Praxis aber dann, wenn nicht einmal eine zureichende Prüfung der Erforderlichkeit und Zulässigkeit der Suchbegriffe vor deren Einsatz stattfindet. Im Nachinein stellte der BND schließlich bei Prüfungen im Sommer 2013 – nach den *Snowden*-Enthüllungen – selbst fest, dass

529) *Süddeutsche.de* vom 30. Oktober 2015, „NSA jubelte BND deutsche Spähziele unter“, http://www.sueddeutsche.de/politik/geheimdienst-affaere-nsa-jubelte-bnd-deutsche-spaehziele-unter-1.2715253, abgerufen am 18. Juni 2017.

mehrere zehntausend NSA-Selektoren unzulässig gewesen waren, da sie sich vor allem gegen Regierungen und Institutionen in den EU-Staaten, gegen EU-Einrichtungen, gegen Deutsche und deutsche Firmen im Ausland gerichtet haben.[530]

aa) Prüfkriterien unzulänglich

Die Zeug_innen des BND haben übereinstimmend angegeben, dass die Prüfung der NSA-Selektoren anfangs ausschließlich anhand sog. G 10-Kriterien erfolgt sei. Damit sind vor allem die deutsche Telefonvorwahl „0049“, die Endung „.de“ bei E-Mail-Adressen und dem BND bekannte Adressen von Deutschen oder deutschen Institutionen im Ausland (z. B. Deutsche Botschaften) gemeint. Während der gemeinsamen Operation seien dann 2005/2006 unter den NSA-Selektoren zufällig Telefonnummern der Firmen *EADS* und *Eurocopter* bemerkt worden, die dann in eine weitere Kategorie von auszusondernden Selektoren gekommen seien (zum Schutz von „deutschen Interessen“).

Selbst der ehemalige BND-Präsident *Schindler* hat die NSA-Selektoren-Prüfung bis August 2013 vor dem Ausschuss scharf kritisiert:

> „Die Überprüfung der Selektoren war von Beginn an unvollständig. Bei Beginn im April 2005 erfolgte ausschließlich eine Überprüfung nach G-10-Kriterien. Die Prüfung war also bereits bei ihrem Start im April unzureichend. Weisungen oder eine Dienstvorschrift zur Umsetzung des MoA von 2002 gab es nicht, nicht im BND und nicht von anderer Stelle. Spätere Überprüfungen der Selektoren mit EU-Bezug erfolgten eher zufällig. Eine systematische Überprüfung ist seit April 2005 nicht erfolgt, und die erste – ich sagte es bereits – erfolgte im August 2013.

530) siehe dazu in Kapitel VIII – BND-Selektoren: Abhören unter Freunden geht wunderbar.

> Dieses von Beginn an unzureichende Verfahren wurde verfestigt mit der Umstellung auf elektronische Prüfung im Juni 2008, quasi maschinell verfestigt, obwohl man vorher suspekte Selektoren festgestellt hatte. Ich kann mir das nicht erklären.“[531]

Auch die BND-Datenschutzbeauftragte, die Zeugin *H. F.*, die nach dem Aufdecken der NSA-Selektoren-Problematik im März 2015 die „Prüfgruppe Selektoren“ geleitet hatte, hat vor dem Ausschuss festgestellt, dass die Prüfung der NSA-Selektoren in der Vergangenheit unzureichend war und den BND-Mitarbeiter_innen andere Kriterien als „G 10“ gefehlt haben:

> „Ich denke, was insgesamt bei der Selektorensteuerung, auch im Hinblick auf die ausländischen Selektoren, ein Problem war: dass die Mitarbeiter wenige Anhaltspunkte hatten: „Linke Grenze, rechte Grenze: Was ist eine zulässige Steuerung? Was ist eine unzulässige Steuerung?“, also: „Wo muss ich aufpassen?“, Stichwort: EU-Ausländer und Ähnliches. Die Mitarbeiter sind sehr intensiv in der Vergangenheit geschult worden zum Thema G 10; aber die sonstigen Interessen, europäische Interessen und Ähnliches, da herrschte offensichtlich Unkenntnis.“[532]

Die seit 2008 von „händisch“ auf automatisiert umgestellte Prüfung der NSA-Selektoren mag das Problem verschärft haben, weil dann nur noch der Computer maschinell die Suchbegriffe nach dem vorgegegebenen Raster durchsucht hat. Der Systemfehler lag aber an den mangelhaften Prüfkriterien. Der BND war auf den sog. G 10-Schutz fixiert, der aber auch nur so gut funktionieren kann, wie es zureichende Erkennungsmerkmale für „deutsche“ Adressen und andere Telekommunikationsmerkmale gibt. Beispielsweise auch in Deutschland verbreitete E-Mail-Adressen von ausländischen Providern wie *gmail.com*, *aol.com*, *yahoo.com* usw. wären ohne Zusatzwissen

531) *Schindler*, Protokoll-Nr. 50 I, S: 76.

532) *H. F.*, Protokoll-Nr. 121 I, S. 24.

zum Inhaber weder händisch noch automatisiert herausgefiltert worden. Bei Selektoren wie Messenger-IDs ist es unmöglich, die Nationalität oder eine geografische Zuordnung festzustellen. Für zahlreiche andere Selektoren-Typen gilt dies ebenso.

Eine Sensibilität für den Schutz von Bürger_innen und Institutionen in EU-Staaten und anderer „deutscher Interessen“ fehlte im BND vollständig. Das mag auch daran gelegen haben, dass der deutsche Auslandsnachrichtendienst selbst in großem Umfang Selektoren von Regierungen und Ministerien der EU-Staaten und Einrichtungen der Europäischen Union einsetzte und diese überwachte (siehe zu den unzulässigen BND-eigenen Selektoren in Kapitel VIII). Der BND sah darin gar nichts Problematisches – bis zu den Aussprüchen der Bundeskanzlerin und ihres Regierungssprechers im Sommer 2013: „Abhören unter Freunden geht gar nicht.“

Völlig unzulänglich war das rein zufällige Aussortieren von unzulässigen oder unerwünschten NSA-Selektoren mit EU-Bezug, von europäischen Firmen oder solchen mit deutscher Beteiligung. Insgesamt untauglich ist auch die Rechtfertigung des BND, bei der Auswertung der „Treffer“ und dem Erstellen der Meldungen seien solch unzulässige Selektoren doch aufgefallen. BND-Zeug_innen haben vielmehr bestätigt, dass sie die mit NSA-Selektoren gewonnenen Daten in der Regel gar nicht gesichtet haben, weil sie mit den eigenen Treffern genug zu tun hatten.[533]

Eine Weisung der Abteilungsleitung oder des Präsidenten für den Einsatz von NSA-Selektoren (oder von anderen Partnerdiensten) gab es bis März 2015 nicht. Das Memorandum of Agreement zwischen BND und NSA, dass die Zwecke der gemeinsamen Fernmeldeaufklärung festhielt und die Aufklärung europäischer Ziele nur unter bestimmten Voraussetzungen gestattete,[534] war den zuständigen Mitarbeiter_innen nur teilweise oder gar nicht bekannt.

Festzustellen ist hier ein seit Beginn der Kooperation durchgängiges Führungsversagen der Abteilungsleitung und des BND-Präsidenten, da abgesehen vom „G 10“-Schutz keine Vorgaben für die Zulässigkeit des Einsatzes der NSA-Selektoren gemacht wurden.

---

533) *R. U.*, Protokoll-Nr. 47 I, S. 22 f.

534) *Schindler*, Protokoll-Nr. 54 I, S. 30.

bb) Riesige Anzahl der NSA-Selektoren unverhältnismäßig und das Problem der Permutationen und Abwandlungen

Ein rechtliches und ein Überprüfungs-Problem stellt auch die große Anzahl der von der NSA gelieferten Selektoren dar. Nach Medienberichten sei der Bestand von anfangs mehreren hunderttausend NSA-Selektoren auf rund 8,2 Millionen im August 2013[535] angewachsen; darunter seien aktive und inaktive – also eingesetzte und nicht eingesetzte – Suchbegriffe gewesen. Im Jahr 2015 habe die Anzahl bei mindestens 14 Millionen NSA-Selektoren gelegen.[536] Im März 2015 hätte der BND davon ca. 4,6 Millionen Suchbegriffe der NSA tatsächlich eingesetzt, die sich auf 1,267 Millionen Personen und Unternehmen bezogen hätten.[537] Bei den Angaben gehen wir davon aus, dass es sich um sog. IP-Selektoren handelt und weitere, jedoch eine deutlich geringere Anzahl, sog. Telefonie-Selektoren hinzukommen.

Selbst wenn man berücksichtigt, dass in den IP-Selektoren der NSA sogenannte Permutationen[538] enthalten sind, stellen rund 1,2 Millionen reale Personen und Unternehmen – nimmt man die Zahlen von März 2015 – eine ungeheure Anzahl von Betroffenen dar.

Die Nutzung der NSA-Selektoren muss – damit sie rechtmäßig ist – auch für die Aufgabenerfüllung des BND erforderlich sein. Es genügt nicht, dass der BND hier eine Art Auftragserfassung für die NSA praktiziert, weil er dies zwecks Kooperation in einem

535) *Zeit Online* vom 19. Mai 2015, „Selbst der BND weiß nicht, was NSA-Selektoren suchen“, http://www.zeit.de/digital/datenschutz/2015-05/bnd-affaere-selektoren-nsa-liste, abgerufen am 18. Juni 2017.

536) *Zeit Online* vom 19. Mai 2015, „Selbst der BND weiß nicht, was NSA-Selektoren suchen“, http://www.zeit.de/digital/datenschutz/2015-05/bnd-affaere-selektoren-nsa-liste, abgerufen am 18. Juni 2017.

537) *Zeit Online* vom 19. Mai 2015, „Selbst der BND weiß nicht, was NSA-Selektoren suchen“, http://www.zeit.de/digital/datenschutz/2015-05/bnd-affaere-selektoren-nsa-liste, abgerufen am 18. Juni 2017.

538) Permutationen seien nach BND-Erläuterung Abwandlungen in der technischen Schreibweise ein und desselben Selektors wegen der bei Internetkommunikation unterschiedlich verwendeten Kodierungsverfahren; beim Permutieren beispielsweise einer E-Mail-Adresse werde das @-Zeichen durch %40 ersetzt; vgl. auch *Graulich*, Bericht vom 23. Oktober 2015, MAT A SV-11/2, S. 25 ff.

MoA so vereinbart hat. Die Kooperation und die vereinbarte Datenübermittlung allein können keine zulässigen Zwecke der Datenerhebung sein.[539]

Aus den Zeugenaussagen ist deutlich geworden, dass der Umfang der NSA-Selektoren den der in der Kooperation genutzten BND-Selektoren um ein Mehrfaches übersteigt. Aus den Aussagen der BND-Zeug_innen ergibt sich zudem, dass der BND, die mit den NSA-Selektoren erzielten „Treffer" aus Kapazitätsgründen überwiegend gar nicht auswertet.[540] Allein das zeigt schon, dass die NSA Selektoren übermittelt hat, an denen der BND in der Regel gar kein Interesse hatte, die also nicht erforderlich im Sinne des § 1 Absatz 2 Satz 1, § 2 Absatz 1 Satz 1 BNDG waren.

Der BND war auch gar nicht in der Lage, einen Umfang von mehreren Millionen NSA-Selektoren daraufhin zu überprüfen, ob ihr Einsatz erforderlich im Sinne der Aufgabennorm des BND ist. Unterstellt, dass für die wöchentlichen Überprüfungen auch nur zehntausend neue NSA-Selektoren angeliefert wurden, stellt sich schon angesichts der Menge die Frage, wie eine Erforderlichkeitsprüfung praktisch umgesetzt werden konnte. (Zu anderen technischen und systemischen Problemen siehe gleich unter cc).)

Ein weiteres Problem ergibt sich im Zusammenhang mit den sogenannten Permutationen der Selektoren. Sofern Permutationen tatsächlich nur die technisch unterschiedliche Schreibweise ein und desselben Selektors aufgrund verschiedener Kodierungsverfahren bei IP-Verkehren sind, wäre dies unbedenklich. Ob dies tatsächlich bei jedem einzelnen Selektor der Fall ist, scheint dem BND jedoch gar nicht bekannt zu sein. Denn der BND weiß nicht, wie die NSA die Permutationen erstellt. Im Bericht von *Graulich* heißt es dazu:

> „Die genaue Zahl der den amerikanischen Selektoren zu Grunde liegenden TKM [Telekommunikationsmerkmale] ist dem BND nicht bekannt. Sie lässt sich mangels Kenntnis des von der NSA verwendeten

539) Im Ergebnis so auch die BfDI in ihrer rechtlichen Bewertung zum Sachstandsbericht vom 30. Juli 2015 unter 1.A.I.2.b), veröffentlicht auf netzpolitik.org, https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/, abgerufen am 30. Mai 2017.

540) *R. U.*, Protokoll-Nr. 47 I, S. 22 f.

> Algorithmus auch nicht zurückrechnen, sondern nur erfahrungswissenschaftlich schätzen.“[541]

Ob ein Selektor danach tatsächlich die Permutation des vermeintlichen Telekommunikationsmerkmals ist, muss der BND der NSA schlicht glauben. Es erscheint sehr fraglich, dass der BND unter diesen Umständen die Zulässigkeit der NSA-Selektoren zuverlässig überprüfen kann.

Die Aussagen von BND-Zeug_innen wecken jedoch noch den weiteren Verdacht, dass neben Permutationen auch andere Verfahren zur Gewinnung von NSA-Selektoren mit enormer Streubreite angewandt wurden und dies von den Zeug_innen möglicherweise irrtümlich als Permutationen bezeichnet wurde. Der Zeuge *H. K.*, Referatsleiter in der Unterabteilung T2, hat vor dem Ausschuss zur Praxis der NSA ausgesagt:

> „Nein, die haben ein anderes Verfahren. Wenn es jetzt zum Beispiel eine bestimmte – – Nehmen wir eine bestimmte E-Mail-Adresse, zum Beispiel, sagen wir mal, sensburg@yahoo.com. Wenn die Amerikaner ziemlich sicher sein wollen, dass sie Sie erfassen wollen, dann decken sie nicht nur die yahoo.com ab, sondern nehmen alle möglichen Permutationen (…) alle möglichen Provider, sodass aus dieser einen Adresse, die de facto real vielleicht existiert, dann Dutzende zusammenkommen.“[542]

Auch der ehemalige BND-Präsident *Schindler* hat sich als Zeuge in dieser Weise geäußert:

> „Telekommunikationsmerkmale bei E-Mail-Adressen weisen dabei unterschiedliche technische Schreibweisen auf, bis zu 20, sogenannte Permutationen. Jede Permutation stellt einen eigenen Selektor dar. Beispiel: „Gerhard Schindler“, „Gerhard.Schindler“, „G. Schindler“, „G. S.“, und welche Variationen man sich auch immer ausdenken kann.

541) *Graulich*, Bericht vom 23. Oktober 2015, MAT A SV-11/2, S. 26.

542) *H. K.*, Protokoll-Nr. 87 – Auszug offen, S. 26.

> Diese hohe Zahl an Permutationen erklärt auch die hohen Zahlen, die zurzeit im Raume stehen.“[543]

Selbst auf ausdrückliche Nachfrage und Vorhalt von Beispielen technisch permutierter Selektoren aus einem BND-Schriftstück[544] blieb *Schindler* bei seiner Aussage:

> „Nein, im Prinzip, Herr Vorsitzender, ist es beides. Ich habe bei dem Beispiel, was ich Ihnen hier mündlich vorgetragen habe, versucht, es so einfach für einen Juristen wie mich wie möglich zu machen. Diese unterschiedlichen Schreibweisen gibt es bei diesen Permutationen, so, wie ich sie dargestellt habe. Es gibt sie aber auch so, wie in dem Testat es dargestellt worden ist. Ich sagte ja, dass wir teilweise bis zu 20 solcher Permutationen zu einem Begriff, zu einem Telekommunikationsmerkmal haben, und da ist es klar, dass es nicht nur um die Schreibweise „G.Schindler“ oder „Gerhard Schindler“ geht, sondern dass es auch eben sonstige technische Änderungen, die ich allerdings nicht verstehe – – Warum „Prozent 2 Punkt sonst was“ da steht – – Aber es sind technische Änderungen, mit denen man ebenfalls Permutationen erzeugen kann. Es ist beides richtig, Herr Vorsitzender.“[545]

Sollte es tatsächlich in dieser Weise generierte NSA-Selektoren geben, wären davon in hohem Maße Personen betroffen, die gar nicht Ziel der Überwachung sind. Für den BND wäre bei einer Prüfung eine etwaige Erforderlichkeit im Einzelfall gar nicht erkennbar. Ein solch ungezielter Einsatz von Selektoren wirft jedoch nicht nur Fragen der Überprüfbarkeit auf, er wäre auch in jedem Fall unverhältnismäßig.

Der Einsatz von NSA-Selektoren in diesem Umfang und unter diesen Umständen ist daher rechtswidrig.

543) *Schindler*, Protokoll-Nr. 50 I, S. 75.

544) Sog. Testat des BND vom 30. April 2015, MAT A BND-26/1 (Tgb.-Nr. 142/15 – GEHEIM).

545) *Schindler*, Protokoll-Nr. 50 I, S. 78.

cc) Fehlende Deutungen und nichtlesbare NSA-Selektoren

Die Beweisaufnahme hat ergeben, dass die NSA-Selektoren zum Teil – möglicherweise zum größeren Teil – gar nicht oder nur sehr beschränkt überprüfbar waren. Unterschiede gab es bei den sog. Telefonie-Selektoren und den Internet-Selektoren (IP-Selektoren), die in verschiedenen Datenbanken in Bad Aibling geführt wurden.

Zum einen bestand das Problem darin, dass die NSA zu den Selektoren oftmals keine Angaben zum Zweck – also eine Begründung für die Steuerung – oder zur überwachten Person/Institution mitlieferte. Der BND nennt diese Angabe „Deutung“. Die Aussagen der Zeug_innen in eingestufter Sitzung und Angaben in den eingestuften Akten zum Vorhandensein solcher Deutungen bei den Telefonie-Selektoren weichen voneinander ab.[546] Möglicherweise beziehen sie sich auf unterschiedliche Zeiträume.

> **[Platzhalter für Wiedergabe der Passagen aus dem eingestuften Protokoll und der Akte aus Fußnote 546.]**

Wir gehen nach Würdigung der Aussagen und der Akten sowie des Berichts von *Graulich* in unserer Bewertung davon aus, dass in den Anfangsjahren (2005-2007) Deutungen mitgeliefert wurden, die Telefonie-Selektoren der NSA zumindest in den letzten Jahren überwiegend keine Deutungen enthalten haben.

Auch hinsichtlich der IP-Selektoren gibt es divergierende Angaben: Der Zeuge *W. O.*, der in Bad Aibling die Aktivierung der NSA-Selektoren nach der Prüfung vorgenommen hat, hat ausgesagt, dass es für IP-Selektoren gar keine Deutungen gegeben habe.[547] Die von der Bundesregierung für die Einsicht in die NSA-Selektorenliste eingesetzte „Sachverständige Vertrauensperson“ *Kurt Graulich* schreibt hingegen in ihrem Bericht:

> „Die an den NSA-Internet-Selektoren vorhandenen Begründungen waren aus informationstechnologischen Gründen für die BND-

546) s. *W. O.*, Protokoll-Nr. 59 II (Tgb.-Nr. 229/15 – GEHEIM), S. 40.; E-Mail von *K. M.* vom 8. November 2013 an *H. K.*, MAT A BND-38b/39b (Tgb.-Nr. 41/15 – STRENG GEHEIM, nur zur Einsicht in der Geheimschutzstelle des Deutschen Bundestages), Ordner 416, Bl. 69.

547) *W. O.*, Protokoll-Nr. 59 I, S. 44.

> Mitarbeiter von Anfang an nicht lesbar, weil NSA und BND mit unterschiedlichen Datenbanksystemen arbeiteten.“[548]

Im Ergebnis ist es einerlei, ob Deutungen und Begründungen gar nicht erst vorhanden oder ob sie nicht lesbar waren.

Ohne eine (lesbare) Deutung ist eine Erforderlichkeitsprüfung und zum Teil sogar eine G 10-Prüfung von Telefonnummern, E-Mail-Adressen, Messenger-IDs etc., deren Inhaber der BND nicht kennt, von vornherein ausgeschlossen. Der für die NSA-Selektorenprüfung zuständige BND-Mitarbeiter *K. M.* hätte wenigstens seine wenn auch unzureichende automatisierte Wortbank-Suche zur G 10-Prüfung und zur rudimentär vorhandenen Überprüfung deutscher Interessen über die Deutungen, die ggf. (Firmen-)Namen, Zusammenhänge oder Steuerungsgründe enthielten, laufen lassen können. Angeblich anhand der Deutungen sollen damals, jedoch noch im „händischen“ Verfahren, die Telefonnummmern von *EADS* und *Eurocopter* aufgefallen sein.

Zum anderen hat die NSA teilweise IP-Selektoren geliefert, die als Selektoren gar nicht erkennbar waren bzw. bei denen nicht erkennbar war, welcher Kommunikationsdienst damit überhaupt erfasst wird. Der Zeuge *H. K.*, Referatsleiter in der Unterabteilung T2 und Vorgesetzter des Zeugen *K. M.*, der für die Selektorenpürfung zuständig war, hat hierzu ausgesagt:

> „Wenn er was nicht erkennen kann als unzulässigen Selektor, weil es bestimmte Kombinationen von Buchstaben und Zahlen sind, dann kann er es auch nicht prüfen.“[549]

Das Problem habe insbesondere bei „neuen Medien“ und immer wieder neu auftretenden Kommunikationstypen (z. B. Messenger-Diensten) bestanden.[550] Außerdem seien Hash-Werte als Selektoren verwendet worden,[551] die der BND nicht nachvollziehen konnte.

---

548) *Graulich*, Bericht vom 23. Oktober 2015, MAT A SV-11/2, S. 208.

549) *H. K.*, Protokoll-Nr. 77 I, S. 33.

550) *K. M.*, Protokoll-Nr. 62, S. 66 f.

551) Details dazu in eingestufter Sitzung, *W. O.*, Protokoll-Nr. 59 II (Tgb.-Nr. 229/15 – GEHEIM), S. 29 f.

Der Zeuge *H. K.*, Referatsleiter T2A und zuständig für das Sachgebiet, das die NSA-Selektoren wöchentlich geprüft hat, räumte in seiner Vernehmung Probleme wegen der Nichtlesbarkeit von Selektoren ein und schilderte die gravierenden Folgen:

> „Was T2A anbetrifft, haben wir da einfach das Problem gehabt, [redacted].“[552]

BND-Zeug_innen haben versucht, das Problem zu relativieren, in dem sie darauf verwiesen haben, dass die NSA-Selektoren in sogenannten Equations geliefert worden seien. Nach Angaben des BND seien in einer „Equation“ zu einem Teilnehmer, sofern vorhanden, mehrere Selektoren gespeichert gewesen, z. B. eine Telefonnummer und eine E-Mail-Adresse.[553] Sobald einer der Selektoren als „geschützt“ erkannt worden sei, sei die gesamte „Equation“ nicht für die Erfassung freigegeben worden.[554]

Dieser vermeintliche Sicherungsmechanismus kann aber selbst nach BND-Logik nur dann funktionieren, wenn in einer „Equation“ in jedem einzelnen Fall neben einem nichtlesbaren Selektor ein lesbarer vorhanden ist, der auch auf „G 10“-Schutz und Erforderlichkeit und Zulässigkeit geprüft werden kann. Beispielsweise müsste zu einem Selektor mit einer unbekannten Ziffernfolge auch ein Telefonnummern-Selektor existieren. Es ist zu bezweifeln, dass dies immer der Fall war.

Da der NSA stets mitgeteilt wurde, welche Selektoren der BND abgelehnt hat, und nichtlesbare Selektoren bis mindestens März 2015 auch nicht von vornherein vom

552) *H. K.*, Protokoll-Nr. 87 (Tgb.-Nr. 269/16 – GEHEIM), S. 34.

553) *W. O.*, Protokoll-Nr. 48 I, S. 12.

554) *W. O.*, Protokoll-Nr. 48 I, S. 15.

BND aussortiert wurden, wäre es für die NSA ein Leichtes gewesen, nichtüberprüfbare Selektoren so zu liefern, dass sie mit hoher Wahrscheinlichkeit nicht abgelehnt worden wären. Entweder als einziger Selektor in der „Equation“ oder quasi verschleiert in einer Equation mit zulässigen Selektoren zu einem anderen Teilnehmer. Ein Vertrauensvorschuss gegenüber der NSA, dass sie hier in jedem Fall vereinbarungsgemäß arbeitet, ist nach den Erfahrungen des BND bei EIKONAL nicht angebracht (siehe hierzu unter V.6 – Zu Risiken und Nebenwirkungen…).

Aufgrund der fehlenden Deutungen und nichtlesbarer oder erkennbarer Selektoren konnte weder ein umfassender G 10-Schutz noch ein Schutz deutscher und europäischer Interessen gewährleistet werden. Auch eine Erforderlichkeitsprüfung ist wegen fehlender Kenntnis darüber, wessen Kommunikation ein Selektor zu welchem Zweck überhaupt erfassen soll, gar nicht erfolgt. Eine derartige Praxis verstößt gegen das BND-Gesetz und das Artikel 10-Gesetz.

Auch die BfDI kommt in ihrer rechtlichen Bewertung zu diesem Ergebnis. In dem auf Netzpolitik.org veröffentlichten Bericht heißt es:

> „Der BND hat seine insoweit bestehende Prüfpflicht nicht erfüllt. Er hat ohne die notwendige positive Erforderlichkeitsprüfung die von der NSA ohne Deutungen übermittelten personenbezogene[n] Selektoren (Sachstandsbericht, B, VI, 3, b, bb, 2) gespeichert und verwendet. Dies ist ein schwerwiegender Verstoß gegen die Vorgaben der § 1 Absatz 2 Satz 1, § 2 Absatz 1 Satz 1 BNDG.“[555]

dd) Fehlende Kontrolle ist schweres Versäumnis der BND-Amtsleitung

Das gesamte Procedere des Einsatzes von NSA-Selektoren durch den BND war schon vom Ansatz her nicht mit dem BND-Gesetz und den Datenschutzbestimmungen vereinbar. Weder die Erforderlichkeit noch die Verhältnismäßigkeit wurden gewahrt.

555) BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015 unter 1.A.I.2.b), veröffentlicht auf netzpolitik.org, https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/, abgerufen am 30. Mai 2017.

Das implementierte Selektoren-Prüfverfahren war ebenfalls vom Ansatz her unzureichend. Es war auf den „G 10“-Schutz fixiert, blieb aber auch dabei unzulänglich. Der Schutz „deutscher Interessen“ war vom Zufall abhängig, der Schutz von EU-Bürger_innen, -Institutionen und Firmen spielte beim BND bis August 2013 gar keine Rolle.

Problematisch ist vor allem, dass die Amtsleitungen, insbesondere die damaligen BND-Präsidenten *Uhrlau* und *Schindler* offenbar keinerlei Vorstellung davon hatten, in welcher Weise und in welchem Umfang der BND mit Suchbegriffen der NSA Telekommunikation überwachte. Ein steuerndes Eingreifen z. B. mit Weisungen blieb daher aus.

Eine laufende Kontrolle des Selektoren-Prüfverfahrens beispielsweise durch Berichtsanforderungen gerade vor dem Hintergrund der technischen Entwicklungen bei der Internetkommunikation fand seitens der Amtsleitung nicht statt.

b) Unzulässige NSA-Selektoren

aa) Aufdeckung der NSA-Selektoren-Problematik

Nur durch einen Beweisantrag der Opposition (Beweisbeschluss BND-26) ist überhaupt bekannt geworden, dass der BND unzulässige NSA-Selektoren eingesetzt und im August 2013 in größerem Umfang aussortiert hat. Ohne diesen Beweisantrag, der am 26. Februar 2015 vom Ausschuss beschlossen wurde, würden heute noch die 40.000 bemakelten NSA-Selektoren in den Datenbanken in Bad Aibling schlummern. Weder das Kanzleramt noch der Ausschuss hätten eine Ahnung davon gehabt. Auch wäre ohne den Beweisantrag die bisherige rechtswidrige Praxis bei Prüfung und Einsatz der NSA-Selektoren fortgesetzt worden. Für die unzulässigen BND-eigenen Selektoren gilt dies in ähnlicher Weise: Der Chef des Kanzleramtes, *Peter Altmaier*, und die Arbeitsebene in der Abteilung 6 wüssten bis heute nicht von den Deaktivierungen und Weisungen im Herbst 2013. Dies ist ihnen angeblich erst bei der Aufdeckung der NSA-Selektoren-Problematik im März 2015 bekannt geworden (s. dazu Kapitel VIII – BND-Selektoren: Abhören unter Freunden geht wunderbar).

Zwar hätten BND und Kanzleramt die NSA-Selektorenlisten auch schon auf den Beweisbeschluss BND-1 vom 10. April 2014 liefern können und müssen. Mit diesem waren alle Unterlagen zum Untersuchungsauftrag, die seit den *Snowden*-Enthüllungen von Anfang Juni 2013 erstellt worden waren, angefordert worden. Irgendwo im BND entschied man aber, diese Unterlagen vorerst zurückzuhalten.

Ein solches Vorgehen bei der Aktenvorlage unterminiert die Rechte des Ausschusses. Ein Untersuchungsausschuss hat das Recht und ist darauf angewiesen, dass ihm die Unterlagen vollständig vorgelegt werden. Er weiß in der Regel nicht, welche Akten im Einzelnen in den Behörden vorhanden sind – selbst nach der Vorlage von Aktenplänen nicht – und kann daher zumeist nur in allgemeiner Form Unterlagen anfordern.

Einen Hinweis auf möglicherweise problematische oder unzulässige NSA-Selektoren und Spionageversuche der NSA gegen deutsche Interessen hat der Ausschuss erstmals Unterlagen zur Operation EIKONAL entnehmen können, die dem Ausschuss im September 2014 zugingen. Im Zuge der Beweisaufnahme verdichteten sich die Hinweise – jedoch ohne, dass BND-Zeug_innen dazu konkrete Angaben gemacht oder irgendeinen Hinweis auf ein Selektoren-Problem in der Vergangenheit gegeben hätten –, sodass die Opposition im Februar 2015 einen entsprechenden Beweisantrag stellte.

bb) *EADS*, *Eurocopter* & Co.: BND war schon 2005/2006 gewarnt – und verschwieg Vorfall gegenüber dem Ausschuss

Bereits im Jahr 2005 hatte der BND Hinweise darauf, dass die NSA Aufklärung gegen deutsche Interessen in der Kooperation bei EIKONAL und in der JSA in Bad Aibling betreibt und unzulässige Selektoren einsteuert. In einem Bericht von *Frontal 21* wird über den Vorfall aus einem BND-Schriftstück von 2010 für den Abteilungsleiter 6 im Kanzleramt, *Günter Heiß*, zitiert:

> „NSA hat jedoch in 2005 Erfassungskriterien zu den Firmen *EADS*, *Eurocopter* und verschiedenen französischen Behörden in JSA (…) eingestellt. BND hat dies entdeckt und im Anschluss unterbunden.“[556]

556) *Frontal 21*, „Nachgehakt“ vom 27.4.2015, „US-Wirtschaftsspionage: de Maiziere war ab Februar 2008 informiert“.

In einer eingestuften E-Mail des BND aus der JSA in Bad Aibling vom 25. Januar 2006, die dem Ausschuss am 28. April 2015 vorgelegt wurde, heißt es zu dem Vorgang:

> „[redacted]“[557]

Als Anlagen zur E-Mail wurden Dateien mit den Selektoren angefügt. Sie sind jedoch von der Bundesregierung aus den Unterlagen entnommen worden, da es sich um Material eines ausländischen Nachrichtendienstes handele.

Aus der E-Mail ergibt sich nicht, dass die unzulässigen Selektoren *vor* der Verwendung entdeckt wurden. So haben es jedoch BND-Zeug_innen vor dem Ausschuss behauptet. Es spricht aufgrund der Formulierung einiges dafür, dass die Selektoren tatsächlich für die Erfassung genutzt wurden und sie erst nachträglich aufgefallen sind. Die von der Bundesregierung eingesetzte „Sachverständige Vertrauensperson“ *Graulich* kam in ihrem Bericht zu dem Ergebnis, dass der genaue Vorgang wegen fehlender Akten nicht mehr rekonstruiert werden könne. *Graulich* notierte:

> „Festgestellt werden konnte lediglich, dass am 25. Januar 2006 von der Dienststelle Bad Aibling bestätigt wurde, dass die Selektoren zu den Firmen *EADS* (52 Rufnummern) bzw. *EUROCOPTER* (22 Rufnummern) nicht mehr für die Erfassungssteuerung verwendet wurden.“[558]

Gegenüber dem Untersuchungsausschuss wurde der *EADS*/*Eurocopter*-Vorfall von BND-Zeugen zunächst verschwiegen. Der Zeuge *T. B.*, der im fraglichen Zeitraum

557) E-Mail vom 25. Januar 2006, MAT A BND-26 (Tgb.-Nr. 37/15 – STRENG GEHEIM; nur zur Einsicht in der Geheimschutzstelle des Deutschen Bundestages), Anl. 01 (Ordner 367), Bl. 1-3 (Bl. 2-3 entnommen wg. AND-Material).

558) *Graulich*, Bericht vom 23. Oktober 2015, MAT A SV-11/2, S. 189.

2005/2006 die JSA geleitet hatte, sprach in seiner Vernehmung am 6. November 2014 selbst *EADS* an:

> „Also, bevor irgendwelche Selektoren eingestellt wurden, wurden diese immer geprüft, damit man einfach diejenigen Selektoren rausgefiltert hat, die rechtlichen Interessen oder eben auch Interessen der Bundesrepublik Deutschland entgegenstanden.
>
> Ein Beispiel dazu ist eine ganz einfache Geschichte: Wenn Sie sagen, es geht ja um deutsche Interessen, aber nicht G 10, dann kann ich Ihnen sagen: *EADS* zum Beispiel ist nur zu 40 Prozent deutsch und unterfällt damit nicht dem G-10-Regime, es wäre aber äußerst dämlich, wenn die Deutschen mit Amerikanern gemeinsam Erfassung zu *EADS* betreiben würden, als unmittelbarem Konkurrenten zu *Boeing*. Nicht, dass es in der Form versucht worden wäre. Ist nicht passiert. Aber das wäre ein typisches Beispiel für deutsche Interessen, die nicht G-10-geschützt sind.“[559]

Selbst nach Vorhalt eines Artikels aus der *Süddeutschen Zeitung* vom 4. Oktober 2014, in dem beschrieben wurde, wie dem BND 2005 aufgefallen sei, „dass die Amerikaner die gemeinsame Arbeit dazu missbrauchten, um nach Informationen über *EADS*, *Eurocopter* und französische Behörden zu suchen,“[560] behauptete der Zeuge *T. B.* in seiner Vernehmung am 6. November 2014, dies sei nur ein „fiktives Beispiel“,[561] und: „Das Beispiel war Theorie.“[562]

Das ist wenig glaubhaft, zumal der Zeuge *T. B.* als JSA-Leiter in der oben zitierten E-Mail als eine der bei dem Vorfall handelnden Personen genannt ist und dieser Vorfall

559) *T. B.*, Protokoll-Nr. 20 I, S. 26.

560) *Süddeutsche Zeitung* vom 4. Oktober 2014, „Codewort Eikonal“.

561) *T. B.*, Protokoll-Nr. 20 I, S. 64.

562) *T. B.*, Protokoll-Nr. 20 I, S. 42.

offenbar wegen seiner Bedeutung über Jahre hinweg bis 2010 Eingang in Unterlagen des BND an das Kanzleramt gefunden hat.[563]

In einer späteren Vernehmung, als die NSA-Selektoren-Problematik aufgedeckt war, entschuldigte *T. B.* seine Aussage mit falschen Erinnerungen: „Das war zu diesem Zeitpunkt nach meiner Erinnerung reine Theorie.“[564] „Also, es war zu diesem Zeitpunkt meine Überzeugung, dass es ein fiktives Beispiel gewesen wäre.“[565] (Zur Vertuschung der NSA-Selektoren-Problematik im Sommer 2013 siehe unter c).)

Aber auch die oben zitierte Aussage des Zeugen *T. B.* von November 2014 zur angeblich umfassenden Prüfung der NSA-Selektoren vor der Einstellung in die Erfassungssysteme nicht nur auf „G 10“ sondern auf „rechtliche Interessen“ und „Interessen der Bundesrepublik Deutschland“ entsprach nicht der Wahrheit. Wie wir festgestellt haben, gab es bis März 2015 außer der „G 10“-Prüfung keine systematische Kontrolle der NSA-Selektoren auf deutsche Interessen, insbesondere nicht auf EU-/NATO-Bezüge (siehe hierzu detailliert unter d)).

cc) Ergebnis der NSA-Selektoren-Untersuchung durch *Graulich*

Die Bundesregierung weigerte sich aus Staatswohlgründen, dem Ausschuss die Liste der ca. 40 000 vom BND als unzulässig aussortierten NSA-Selektoren vorzulegen. Anstelle der Vorlage setzte die Bundesregierung den ehemaligen Bundesverwaltungsrichter *Kurt Graulich* als „Sachverständige Vertrauensperson“ ein, die die NSA-Selektoren sichten und bewerten sollte. Die Opposition hat dieses Verfahren abgelehnt und bestand auf eine eigene Inaugenscheinnahme der Selektoren. Eine Klage vor dem Bundesverfassungsgericht scheiterte bedauerlicherweise (zur grundsätzlichen Kritik an der Verweigerung und am Verfahren siehe Kapitel I – Bewertungen und Anmerkungen zum Verfahren dort g), h), i)).

563) Vgl. MAT A BND-9/6 (Tgb.-Nr. 20/14 – STRENG GEHEIM, pauschal herabgestuft auf GEHEIM, nur zur Einsicht in der Geheimschutzstelle des Deutschen Bundestages), Anl. 10, Ordner 193, Bl. 1-5; MAT A BK-14/1a (Tgb.-Nr. 139/15 – GEHEIM), Anl. 08, Ordner 364, Bl. 5.

564) *T. B.*, Protokoll-Nr. 59 I, S. 75.

565) *T. B.*, Protokoll-Nr. 59 I, S. 91.

Graulich hat bei seiner Untersuchung eine Liste der vom BND seit 2005 bis zum 4. März 2015 aussortierten NSA-Selektoren vorgelegen. Sie soll 39 082 Selektoren umfasst und 2 918 Telefonie-Selektoren und 36.164 Internet-Selektoren enthalten haben. [566] Darüberhinaus betrachtete *Graulich* eine Liste aus dem Jahr 2005 mit den bereits erwähnten 73 Telefonnummern zu *EADS* und *Eurocopter* sowie eine weitere im BND nachträglich gefundenene Liste mit 444 Selektoren aus dem Zeitraum November 2006 bis März 2008.[567] Sie addierten sich jedoch nicht vollständig zu den knapp 40 000 Selektoren hinzu, da sie teilweise in ihnen enthalten waren (offenbar hatte die NSA sie erneut dem BND geliefert).

Die knapp 40 000 Selektoren betrafen wegen der Permutationen bei IP-Selektoren über 7 000 verschiedene Telekommunikationsmerkmale (TKM).[568]

Von den knapp 40 000 NSA-Selektoren hat der BND ungefähr 25 000 im Sommer 2013 aussortiert.[569] Wir gehen daher davon aus, dass wenigstens diese 25 000 Selektoren tatsächlich für die Erfassung von Telekommunikation verwendet wurden, sie also aktiv geschaltet waren. Denn sie wurden erst unter Anwendung des neuen Kriteriums EU-Regierungen und EU-Institutionen herausgesucht, ein Kriterium, das es für die händische und automatisierte Prüfung vorher nicht gab. Das deckt sich auch mit den Befunden von *Graulich*. Unter den übrigen 15.000 Selektoren, die zwischen 2005 und Sommer 2013 aussortiert wurden, sind vor allem solche, die vor der Verwendung ausgefiltert wurden, weil z. B. der „G 10“-Filter anschlug.

Welche Selektoren im Einzelnen auf der Liste standen, hat der Ausschuss nicht erfahren. Nicht einmal welche Staaten und welche EU-Institutionen betroffen waren. Die Bundesregierung hat *Graulich* für die Erstellung der offenen und streng geheim eingestuften Fassungen des Berichts,[570] die dem Ausschuss übermittelt wurden, Vorgaben

566) *Graulich*, Bericht vom 23. Oktober 2015, MAT A SV-11/2, S. 101.

567) *Graulich*, Bericht vom 23. Oktober 2015, MAT A SV-11/2, S. 127.

568) Vgl. *Graulich*, Bericht vom 23. Oktober 2015, MAT A SV-11/2, S. 205.

569) Frankfurter Allgemeine Zeitung Online vom 8. Mai 2015, „BND lehnte sogar 25.000 Suchanfragen ab“, http://www.faz.net/aktuell/politik/inland/bnd-lehnte-sogar-25-000-suchanfragen-der-nsa-ab-13583069.html, abgerufen am 18. Juni 2017.

570) *Graulich*, Bericht vom 23. Oktober 2015, MAT A SV-11/2 (offene Fassung); MAT A SV-11/1 (Tgb.-Nr. 43/15 – STRENG GEHEIM, nur zur Einsicht in der Geheimschutzstelle des Deutschen Bundestages).

gemacht, die eine konkrete Darstellung untersagten. Selbst in der streng geheim eingestuften Fassung finden sich keine genauen Angaben zu den Selektoren.

aaa) Spionage gegen Regierungsstellen von EU-Staaten und Einrichtungen der EU sowie G 10-Verstöße

Das von *Graulich* festgestellte Ergebnis hinsichtlich der NSA-Selektoren ist verheerend sowohl für die NSA als auch für den BND.

Ca. 70 Prozent der aussortierten 40.000 NSA-Selektoren betrafen nach *Graulichs* Feststellungen Regierungsstellen von EU-Staaten und EU-Stellen.[571] Für diese Selektoren gibt *Graulich* an, dass sie zu 99 Prozent auch tatsächlich „gesteuert" waren, also für die Erfassung genutzt wurden, und fast alle „langfristig".[572] Das erklärt sich daraus, dass diese Kategorie von Selektoren bis August 2013 vom BND nicht beanstandet und deshalb auch nicht herausgefiltert worden war.

Rund 25 Prozent der aussortierten Selektoren betrafen Deutschland zugeordnete Telekommunikationsmerkmale (TKM) und Deutsche im Ausland (auch EU); der kleine Rest betraf Nicht-Deutsche und ausländische juristische Personen im Ausland.[573]

Selbst die Selektoren von Teilnehmer_innen in Deutschland oder mit deutschen TKMs, deren gezielte Erfassung durch die Vereinbarung im MoA ausgeschlossen war, wurden zu knapp einem Drittel tatsächlich aktiv gesteuert – wenn auch überwiegend nur kurzfristig.[574] Das zeigt, dass der „G 10"-Filter offenbar nicht hinreichend funktioniert hat. Die Verwendung dieser Selektoren stellt in jedem Fall eine Grundrechtsverletzung dar.

Die Darstellung der Ausschussmehrheit in ihrer Bewertung ist zu diesem Punkt unzutreffend und irreführend, sofern sie bezogen auf die Gesamtmenge der aussortierten NSA-Selektoren behauptet, „dass der ganz überwiegende Teil abgelehnter Selektoren

---

571) *Graulich*, Bericht vom 23. Oktober 2015, MAT A SV-11/2, S. 172; der Anteil bei den TKMs beträgt 62 Prozent Regierungsstellen der EU-Staaten und 7 Prozent EU-Stellen, ebd., S. 174.

572) *Graulich*, Bericht vom 23. Oktober 2015, MAT A SV-11/2, S. 181 f.; „kurzfristig" definiert *Graulich* im Gegensatz dazu als zwischen 7 und 100 Tagen gesteuert, ebd., S. 175.

573) *Graulich*, Bericht vom 23. Oktober 2015, MAT A SV-11/2, S. 172.

574) *Graulich*, Bericht vom 23. Oktober 2015, MAT A SV-11/2, S. 176.

nie aktiv für die Erfassung genutzt wurde. Etwa 21 % waren kurzfristig, nur 10 % länger gesteuert.“[575] Ausweislich *Graulichs* Bericht[576] bezieht sich dies wie oben dargestellt auf die aktive Steuerung deutscher Telekommunikationsmerkmale (ca. ein Drittel). Im Ergebnis muss man zum gegenteiligen Schluss kommen: Der überwiegende Teil der herausgenommenen, bemakelten NSA-Selektoren war aktiv gesteuert und dies für einen längeren Zeitraum.

Verantwortlich für die Grundrechtsverletzungen und Gesetzesverstöße ist der BND, der die Selektoren in seine Erfassungssysteme eingestellt hat. Die NSA hat gegen das MoA verstoßen, in dem sie unzulässige Selektoren dem BND übermittelte. Dass die gesamte Erfassung außerhalb des G 10-Regimes – unabhängig vom Einsatz der NSA-Selektoren – ohne Rechtsgrundlage standfand und damit rechtswidrig war, wurde weiter oben (siehe Kapitel V.3) bereits erörtert.

Das Ausspähen der Kommunikation von Regierungsstellen von EU-Mitgliedstaaten und von Einrichtungen der EU hat sowohl gegen das MoA als auch gegen das Auftragsprofil der Bundesregierung (APB) verstoßen.

Nach dem MoA dürfen europäische Ziele nur sehr eingeschränkt zu bestimmten Phänomenbereichen aufgeklärt werden. Und zwar lediglich im Einzelfall und wenn tatsächliche Anhaltspunkte dafür vorlagen, dass das „Ziel“ in Terrorismus, Drogenhandel oder Proliferation verwickelt war.[577]

Dem Wortlaut des MoA nach kann das in keinem Fall bedeuten, dass man beispielsweise die EU-Kommission oder Mitarbeiterinnen des französischen Außenministeriums ausspioniert, weil man sich dort interessante Informationen über Terrorismus im Land XY verspricht. Ein solches Vorgehen ist eine Pervertierung des Informationsbeschaffungsauftrags und unter keinen Umständen gerechtfertigt. Auch vom APB, das den Auftrag aus dem BND-Gesetz konkretisiert und für den BND bei jeder Informationsbeschaffung bindend ist, ist eine solche Steuerung nicht gedeckt.

---

575) Bewertung der Ausschussmehrheit, Entwurf, A-Drs. 587, S. 81, Zeile 12-14.

576) *Graulich*, Bericht vom 23. Oktober 2015, MAT A SV-11/2, S. 176.

577) So auch *Graulich*, Bericht vom 23. Oktober 2015, MAT A SV-11/2, S. 84; s. a. *Schindler*, Protokoll-Nr. 54 I, S. 30, der auf den Annex I des MoA und dort die Nummer 1.3.2 verweist.

Auch *Graulich* bewertet eine derartige Verwendung EU-bezogener Selektoren als unzulässig:

> „Die Betrachtung im Einzelnen hat erbracht, dass sie sich zum allergrößten Teil auf Regierungseinrichtungen beziehen, die unter keinem denkbaren Gesichtspunkt in der erfolgten Breite hätten aufgeklärt werden dürfen.“[578]

> „Die Aufnahme der E-Mail-Adressen ganzer Bürostäbe europäischer Regierungen ist ein offensichtliches Übermaß, das nicht vom MoA gedeckt ist.“[579]

Graulich erhebt gegenüber der NSA schwere Vorwürfe: Die Verstöße seien „bündnispolitisch prekär“, da die „NSA (…) auf diese Weise aus der Tarnung des Gemeinschaftsprojekts nachrichtendienstliche Aufklärung gegen Mitgliedsländer der Europäischen Union unternommen“ habe.[580]

Gegenüber dem BND ist die „Sachverständige Vertrauensperson“ der Bundesregierung hingegen milde. Durch eine von *Graulich* erdachte, rechtlich aberwitzige Konstruktion des MoA als eine Art Durchleitungsvertrag für Daten an die NSA, sieht er keine Verletzungen deutschen Rechts – nicht einmal bei deutschen Grundrechtsträgern.[581] Der BND hatte danach gar nichts damit zu tun: Die NSA-Selektoren gehörten rechtlich der NSA, die für sie verantwortlich war. Etwaige (Grund-)Rechtsverstöße realisierten sich allenfalls in den USA bei Kenntnisnahme der Daten. Der BND stellte nur als „Carrier“ ein automatisiertes System der Datendurchleitung zur Verfügung.[582]

578) *Graulich*, Bericht vom 23. Oktober 2015, MAT A SV-11/2, S. 186.

579) *Graulich*, Bericht vom 23. Oktober 2015, MAT A SV-11/2, S. 207.

580) *Graulich*, Bericht vom 23. Oktober 2015, MAT A SV-11/2, S. 212.

581) *Graulich*, Bericht vom 23. Oktober 2015, MAT A SV-11/2, S. 194.

582) *Graulich*, Bericht vom 23. Oktober 2015, MAT A SV-11/2, S. 193 f.

Unter datenschutzrechtlichen Gesichtspunkten ist *Graulichs* Auslegung abwegig und unhaltbar. Wie rechtsirrig *Graulichs* Einordnung ist, lässt sich in der fundierten rechtlichen Bewertung der BfDI über den Kontrollbesuch in Bad Aibling nachlesen.[583]

Auch die ehemalige Leiterin des Rechtsreferats (601) der Abteilung 6 im Kanzleramt, die Zeugin *Christina Polzin*, lehnte *Graulichs* Auffassung ab:

> „Also, ehrlich gesagt habe ich diese Rechtsmeinung von Herrn *Graulich* bisher nicht in dieser Ausführung gekannt. Wenn Sie mich dazu fragen, finde ich das kreativ. Ich glaube, ich würde mich jetzt spontan dieser Rechtsauffassung ehrlich gesagt nicht anschließen, weil ich immer noch der Meinung bin, dass Daten, personenbezogene oder personenbeziehbare Daten, die wir in Deutschland erheben, hier unserem Rechtsregime unterliegen und natürlich das Recht auf informationelle Selbstbestimmung hier eine Rolle spielt. Deswegen würde ich jetzt spontan diesen Weg nicht sofort mitgehen. (…) Aber er ist auf jeden Fall kreativ.“[584]

Das Ergebnis von *Graulichs* Untersuchung beweist letztlich, dass alle Schwüre, die NSA würde sich in Deutschland an geltendes Recht halten, falsch und gelogen waren und die NSA vertragsbrüchig war.

bbb) *Graulichs* blinde Flecken und Kurzschlüsse

Graulich bewertete das Ergebnis in seinem Bericht als „qualitativ gravierende Verstöße durch die NSA“. Quantitativ läge die Zahl der Vertragsverletzungen jedoch nur im Promillebereich.[585] Inwiefern solche Aussagen über die Quantität zutreffen, konnte *Graulich* zu diesem Zeitpunkt und aufgrund der Anlage der Untersuchung gar nicht seriös beurteilen. Die aussortierten NSA-Selektoren spiegelten mit Stand 4. März 2015 den damaligen Problemhorizont des BND wieder. Zum einen kennen wir nicht die genauen

---

583) siehe BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015 unter 1.A.I.2.b), veröffentlicht auf netzpolitik.org, https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/, abgerufen am: 30. Mai 2017.

584) *Polzin*, Protokoll-Nr. 72 I, S. 158.

585) *Graulich*, Bericht vom 23. Oktober 2015, MAT A SV-11/2, S. 211.

Herausnahmekriterien insbesondere von August 2013, außer dass nach Zeugenaussagen nach bestimmten E-Mails-Domains von Regierungsstellen europäischer Staaten gesucht worden sein soll. *Graulich* beschrieb die Kriterien in seiner Aussage vor dem Ausschuss als „Regierungsadressen von europäischen Regierungen, von EU-Einrichtungen und Parlament, also Abgeordneten."[586]

Dass die Suchkriterien umfassend und ausreichend waren, ist nach Kenntnis der BND-eigenen Selektoren, die der Ausschuss einsehen konnte, zu bezweifeln, da sehr unterschiedliche recherchierbare Begriffe in den E-Mails-Domains verwendet werden können. Die in den Medien wiedergegebenen Begriffe wie „diplo", „gov" und „Bundesamt", nach denen in Bad Aibling Mitte August 2013 in den NSA-Selektoren gesucht wurde,[587] sind jedenfalls unzureichend. Hinzu kommt das Problem der nichtlesbaren Selektoren. Auch die erst später erfolgten Filter-Anpassungen und die weiteren Suchläufe in den NSA-Selektorenbeständen in Bad Aibling nach März 2015 deuten darauf hin, dass die Herausnahmekriterien im Sommer 2013 unzulänglich waren.

Inwiefern die NSA Wirtschaftsspionage gegen deutsche und europäische Firmen betrieben oder zu betreiben versucht hat, konnte durch die Untersuchung von *Graulich* nicht geklärt werden. Eine Entwarnung – wie von interessierten Kreisen nach einer PKGr-Sitzung gegenüber den Medien behauptet wurde[588] – ist aber keinesfalls angebracht. Zum einen fand *Graulich* in den aussortierten NSA-Selektoren „eine ganze Anzahl, die auf wirtschaftlich tätige Unternehmen mit Sitz in Deutschland oder deutschem Ursprung gerichtet waren."[589]

Zum anderen hatte der BND bislang gar nicht gezielt nach europäischen Firmen in den NSA-Selektoren gesucht und diese daher gar nicht als bemakelt aussortiert. *Graulich* räumte in seiner Vernehmung vor dem Ausschuss auf die Frage, ob denn europäische

---

586) *Graulich*, Protokoll-Nr. 69 I, S. 98.

587) *Süddeutsche Zeitung* vom 2. Mai 2015, „Die Überwachungsfabrik".

588) *Süddeutsche.de* vom 6. Mai 2015, „Angeblich keine Unternehmen auf 2000-er-Liste der NSA-Suchbegriffe", http://www.sueddeutsche.de/news/politik/geheimdienste-angeblich-keine-unternehmen-auf-2000-er-liste-der-nsa-suchbegriffe-dpa.urn-newsml-dpa-com-20090101-150506-99-09271, abgerufen am 18. Juni 2017.

589) *Graulich*, Bericht vom 23. Oktober 2015, MAT A SV-11/2, S. 188.

Firmen überhaupt aus den Selektoren herausgenommen wurden bzw. nach ihnen gesucht wurde, auch ein:

> „Na ja, das europäische Thema kam ja erst später auf, und europäische Firmen wurden sehr reduziert herausgenommen, weil der Ausgangspunkt war ja nicht Schutz europäischer Firmen, sondern Schutz europäischer Regierungseinrichtungen.“[590]

> „Ja, europäische Unternehmen in der Weise nicht; das war ja nicht der Punkt. Also, es wurden bestimmte – – Also, ich komme jetzt immer wieder auf dieselben; aber der Vorrat an Selektoren ist ja irgendwie begrenzt. Aber es wurde keine – – Es wurden ja nicht systematisch europäische Firmen jetzt „unter Schutz gestellt“ in Anführungszeichen.“[591]

Zudem verwenden Firmen oftmals gar keine Top-Level-Domain des Herkunftsstaates, sondern eine .com-Adresse. Schon aus diesem Grund fielen sie nicht in ein mögliches europäisches Such-Raster.

c) Vertuschung der NSA-Selektorenfunde im Wahljahr 2013

Nach der Beweisaufnahme ist die vom Unterabteilungsleiter T2, dem Zeugen *D. B.*, veranlasste außerplanmäßige Prüfung des NSA-Selektorenbestandes und das Auffinden der großen Anzahl unzulässiger NSA-Selektoren im August 2013 weder an den Abteilungsleiter TA, *Pauland*, noch an die Hausleitung bzw. Präsident *Schindler* gemeldet worden. Ebensowenig ist das Kanzleramt als aufsichtsführende Behörde darüber unterrichtet worden. Erst angeblich im März 2015, als die Akten zur Vorlage für den Beweisbeschluss BND-26 zusammengestellt wurden, seien der Präsident und das Kanzleramt über die damaligen NSA-Selektorenfunde aus dem Sommer 2013 informiert worden.

---

590) *Graulich*, Protokoll-Nr. 69 I, S. 90.

591) *Graulich*, Protokoll-Nr. 69 I, S. 98.

Aus den Zeugenaussagen und der Auswertung der Akten ergibt sich, dass mindestens folgende neun Personen im BND von der Sonderprüfung von August 2013 und dem Auffinden der unzulässigen NSA-Selektoren vor März 2015 gewusst haben:

D. B., Unterabteilungsleiter T2, gab die Prüfung Ende Juli/Anfang August 2013 in Auftrag und informierte darüber den Unterabteilungsleiter T1, *W. K.*

Dr. M. T. (Referent bei T2A) untersuchte das NSA-Selektorenprofil und meldete ein Zwischenergebnis am 9. August 2013 an seinen Vorgesetzten *H. K.* (Referatsleiter T2A) und an *D. B.*

D. B. rief daraufhin *R. U.* an, Dienststellenleiter der Außenstelle Bad Aibling, und informierte ihn telefonisch über den Fund zahlreicher NSA-Selektoren, die europäische Regierungsstellen betrafen. *R. U.* unterrichtete seinen Sachbearbeiter *W. O.*, der am 14. August 2013 eine Recherche in den NSA-Selektoren in der Datenbank in Bad Aibling durchführte und rund 12 000 Merkmale auf Anweisung von *R. U.* „löschte".[592] Bei weiteren Suchen in den darauffolgenden drei Wochen deaktivierte *W. O.* aufgrund eigener Kriterien weitere NSA-Selektoren.[593]

D. B. informierte schießlich den Unterabteilungsleiter T1, *W. K.*, über das Ergebnis der NSA-Selektorenprüfung.[594]

Nach der Aussage von *Dr. M. T.* seien noch zwei weitere Sachbearbeiter aus seinem Referat anfangs an der Prüfung beteiligt gewesen. Diese konnten die Untersuchung der NSA-Selektoren aufgrund der Datenmengen aber nicht durchführen.[595]

Der Zeuge *T. B.*, damals Leiter des Sachgebiets T2AB, in dem die NSA-Selektoren standardmäßig geprüft wurden, gab an, dass er wegen Urlaubs erst „im Herbst 2013" von der Untersuchung und „Löschaktion" bei den NSA-Selektoren erfahren habe.[596] *D. B.* gab an, ihn informiert zu haben.[597]

---

592) *Süddeutsche Zeitung* vom 2. Mai 2015, Die Überwachungsfabrik".

593) *W. O.*, Protokoll-Nr. 48 I, S. 66.

594) *D. B.*, Protokoll-Nr. 48 I, S. 121.

595) *Dr. M. T.*, Protokoll-Nr. 47 I, S. 100.

596) *T. B.*, Protokoll-Nr. 59 I, S. 81.

597) *D. B.*, Protokoll-Nr. 48 I, S. 49.

Der Abteilungsleiter TA, *Hartmut Pauland*, war krankheitsbedingt im August 2013 nicht im Dienst; *D. B.* vertrat ihn in dieser Zeit.[598]

aa) Unterlassene Meldung an Vorgesetzte durch Unterabteilungsleiter

Die beiden Unterabteilungsleiter T2 und T1, *D. B.* und *W. K.*, unterließen es pflichtwidrig, ihre Vorgesetzten über den brisanten Fund der unzulässigen NSA-Selektoren zu unterrichten. Gerade vor dem Hintergrund der zeitgleichen Debatte um die Snowden-Enthüllungen und den Verdacht, die NSA spioniere Partnerstaaten und EU-Institutionen aus, hätte umgehend der Abteilungsleiter – und bei dessen Abwesenheit – der Präsident unterrichtet werden müssen. Die Selektorenfunde waren unzwefelhaft ein „besonderes Vorkommnis“, das nach den Dienstvorschriften des BND gemeldet werden musste. *D. B.* und *W. K.* waren beide für eine solche Informationsweitergabe verantwortlich. In *D. B.*s Verantwortungsbereich fand die NSA-Selektorenprüfung statt; in *W. K.*s Verantwortungsbereich liegt die Außenstelle Bad Aibling.

Auf Fragen, warum *D. B.* die Selektorenfunde im Sommer 2013 nicht nach oben gemeldet habe, berief er sich vor dem Ausschuss auf sein Auskunftsverweigerungsrecht. *D. B.* gab lediglich an, er habe keine Relevanz dafür gesehen, den Vorgang nach oben zu melden.[599] Mit der Kenntnis von heute würde er anders handeln; er sieht in dem Versäumnis einen „objektiven Fehler“.[600]

W. K. hat die alleinige Verantwortung auf *D. B.* geschoben; für ihn sei „keine Brisanz erkennbar“ gewesen.[601]

Auffällig ist, dass über den Prüf- und Löschvorgang im August 2013 – abgesehen von der nachträglich aus der Datenbank in Bad Aibling extrahierten Ablehnungsliste der NSA-Selektoren und drei wiederaufgefundenen E-Mails – keine Unterlagen im BND (mehr) existieren. Aufträge, Weisungen und Ergebnismeldungen wurden nach Zeugenaussagen fast ausschließlich mündlich übermittelt. Dies unterstützt die These einer

598) *D. B.*, Protokoll-Nr. 47 II – Auszug offen, S. 40 f.

599) *D. B.*, Protokoll-Nr. 47 I, S. 51.

600) *D. B.*, Protokoll-Nr. 47 I, S. 65, 113.

601) *W. K.*, Protokoll-Nr. 48 I, S. 77.

gezielten Vertuschung. Solch gravierende Vorgänge nicht zu verschriftlichen, ist ebenfalls ein schweres Versäumnis: Es verunmöglicht die Dienst- und Fachaufsicht. Der Vorgang war dadurch für niemandem im BND nachvollziehbar. Möglicherweise war genau dies so gewollt.

bb) Schweigen ist Gold

Angesichts der damaligen öffentlichen Diskussion um die Snowden-Dokumente ist es kaum vorstellbar, die beiden BND-Unterabteilungsleiter *D. B.* und *W. K.* hätten den Vorgang lediglich falsch eingeschätzt und daher nicht nach oben gemeldet. Der Juli 2013 war geprägt von Enthüllungen über NSA-Spionage gegen Partnerstaaten. Ende Juni/Anfang Juli berichteten *Der Spiegel* und der britische *Guardian* darüber, wie die NSA diplomatische Vertretungen europäischer Staaten und der EU verwanzt und ausgespäht habe.[602] Regierungssprecher *Seibert* nahm diese Berichte zum Anlass, auf der Regierungspressekonferenz vom 1. Juli 2013 eine solche Überwachung scharf zu kritisieren:

> „Wenn sich aber bestätigt, dass tatsächlich diplomatische Vertretungen der Europäischen Union und einzelner europäischer Länder ausgespäht worden sind, dann müssen wir ganz klar sagen: Abhören von Freunden ist inakzeptabel. Das geht gar nicht. Wir sind nicht mehr im kalten Krieg.“[603]

Auch Bundeskanzlerin *Angela Merkel* hat sich auf der Sommerpressekonferenz am 19. Juli 2013 in gleicher Weise geäußert:

> „Um jetzt noch einmal klar etwas dazu zu sagen, was wir über angebliche Überwachungen auch von EU-Einrichtungen usw. gehört haben:

---

602) *Spiegel Online* vom 29. Juni 2013, „NSA horcht EU-Vertretungen mit Wanzen aus“, http://www.spiegel.de/netzwelt/netzpolitik/nsa-hat-wanzen-in-eu-gebaeuden-installiert-a-908515.html, abgerufen am 18. Juni 2017; *The Guardian* vom 30. Juni 2013, „New NSA leaks show how US is bugging its European allies“, https://www.theguardian.com/world/2013/jun/30/nsa-leaks-us-bugging-european-allies, abgerufen am 18. Juni 2017; *Der Spiegel* vom 1. Juli 2013, „Angriff aus Amerika“.

603) Mitschrift der Regierungspressekonferenz vom 1. Juli 2013, http://www.schattenblick.de/infopool/parl/fakten/pafp0628.html, abgerufen am 5. Juni 2017.

> Das fällt in die Kategorie dessen, dass man das unter Freunden nicht macht. Das geht nicht.“[604]

Alle großen Print- und Online-Medien berichteten damals über die Äußerungen der Bundesregierung.[605] Das wird auch den beiden Unterabteilungsleitern im BND nicht entgangen sein. Vermutlich war es sogar Auslöser dafür, überhaupt erstmals das NSA-Selektoren-Profil genauer zu betrachten.[606]

Dann jedoch stellte sich am 12. August 2013 der damalige Chef des Kanzleramtes, *Ronald Pofalla*, nach der Sitzung des Parlamentarischen Kontrollgremiums vor die Kameras und erklärte die NSA-Affäre sechs Wochen vor der Bundestagswahl für beendet: Die Vorwürfe seien haltlos und „vom Tisch“:

> „Die NSA hat uns schriftlich versichert, dass sie Recht und Gesetz in Deutschland einhält. Ich zitiere aus einem NSA-Papier, das uns zu den Gesprächen in Washington übermittelt worden ist: ‚Die NSA hält sich an alle Abkommen, die mit der deutschen Bundesregierung, vertreten durch die deutschen Nachrichtendienste, geschlossen wurden, und hat sich auch in der Vergangenheit stets daran gehalten.‘ Bereits in einem Memorandum of Agreement zwischen der NSA und den BND vom 28. April 2002 hat die NSA versichert, und ich muss wieder zitieren: ‚Die NSA erklärt ihr Einverständnis, sich an die deutschen Gesetze und Bestimmungen zu halten, die die Durchführung von Fernmelde- und elektronischer Aufklärung und Bearbeitung in Deutschland regeln.‘ Am 23. Juli dieses Jahres hat uns die NSA schriftlich zuge-

---

604) Mitschrift der Sommerpressekonferenz von Bundeskanzlerin *Merkel* vom 19. Juli 2013, http://archiv.bundesregierung.de/ContentArchiv/DE/Archiv17/Mitschrift/Pressekonferenzen/2013/07/2013-07-19-merkel-bpk.html, abgerufen am 5. Juni 2017.

605) Beispielhaft: *Süddeutsche.de* vom 1. Juli 2013; Zeit Online vom 1. Juli 2013; *Bildzeitung* vom 2. Juli 2013; *Süddeutsche Zeitung* vom 2. Juli 2013; *Frankfurter Allgemeine* vom 2. Juli 2013; *Welt Online* vom 13. Juli 2013; *Spiegel Online* vom 19. Juli 2013; n-tv vom 19. Juli 2013.

606) So auch *Graulich*, der die Berichterstattung über NSA-Lauschangriffe auf EU-Vertretungen Ende Juni 2013 sowie die Berichte über die Erhebung von Millionen von Telefon- und Internetverbindungen Deutscher durch die NSA Ende Juli 2013 als Anlass ausmacht, siehe: *Graulich*, Bericht vom 23. Oktober 2015, MAT A SV-11/2, S. 104.

> sagt: ‚Die NSA unternimmt nichts, um deutsche Interessen zu schädigen.‘ Das bedeutet, unsere zentrale Forderung, dass auf deutschem Boden deutsches Recht eingehalten werden muss, wird demnach durch die NSA erfüllt. Das haben wir jetzt nicht nur mündlich, sondern auch noch einmal schriftlich bestätigt bekommen.“[607]

Auch darüber berichteten die Medien ausgiebig. Dass das alles nur Makulatur war, wusste *D. B.* noch in derselben Augustwoche 2013 – seiner Zeugenaussage nach vermutlich spätestens am 13. August.[608] An jenem Tag kam *Dr. M. T.*, den er mit der NSA-Selektorenprüfung beauftragt hatte, mit einer Selektoren-Liste zu ihm. Die Liste enthielt annähernd 2.000 E-Mail-Adressen von europäischen Regierungseinrichtungen sowie EU-Stellen.[609] Diese Liste belegte, dass sich die NSA weder an das MoA noch an deutsches Recht gehalten hat und ihr deutsche Interessen ziemlich gleichgültig waren. Das vollmundige Statement von *Pofalla* wäre bei Bekanntwerden der NSA-Selektorenfunde wie ein Kartenhaus in sich zusammengefallen, die Behauptungen des Kanzleramtsministers wären widerlegt gewesen – und das so kurz vor der Bundestagswahl.

Wie bereits erwähnt wollte sich Unterabteilungsleiter *D. B.* nicht zu seinem Motiv äußern, warum er die Selektoren-Funde gegenüber Vorgesetzten verschwiegen habe. Ob es tatsächlich so war und BND-Präsident *Schindler* und das Kanzleramt im Sommer 2013 nichts von der NSA-Selektorenproblematik gewusst haben, wissen wir nicht. Fest steht nur, dass damals weder die Öffentlichkeit noch der Bundestag und das Parlamentarische Kontrollgremium über die unzulässigen NSA-Selektoren informiert wurden.

Das Kanzleramt hat am 23. April 2015, dem Tag, an dem es dem Ausschuss und dem Parlamentarischen Kontrollgremium erstmals vom Auffinden der NSA-Selektorenlisten

---

607) Pressestatement von Kanzleramtsminister *Pofalla* nach der Sitzung des Parlamentarischen Kontrollgremiums am 12. August 2013, https://www.bundesregierung.de/ContentArchiv/DE/Archiv17/Mitschrift/Pressekonferenzen/2013/08/2013-08-12-pofalla.html, abgerufen am 5. Juni 2017.

608) *D. B.*, Protokoll-Nr. 47 II – Auszug offen, S. 33.

609) *Graulich*, Bericht vom 23. Oktober 2015, MAT A SV-11/2, S. 127: „Es handelt sich um europäische E-Mail-Adressen, unter denen sich die Namen zahlreicher Mitglieder europäischer Regierungen sowie deren Mitarbeiter befinden. Außerdem enthält sie Namen von Parlamentsabgeordneten und sonstiger öffentlicher Dienststellen aus solchen Ländern.“

berichtete, eine scharf formulierte Pressemitteilung veröffentlicht und dem BND darin „technische und organisatorische Defizite“ bescheinigt.[610]

Dennoch wurden gegen keinen der damaligen Beteiligten im BND bislang ein Disziplinarverfahren eingeleitet oder andere Maßnahmen ergriffen, obwohl der ehemalige BND-Präsident *Schindler* und das Kanzleramt heute der Auffassung sind, dass dieser Vorgang gravierend war und damals nach oben hätte gemeldet werden müssen.

cc) Fragen ist Silber: Versäumnisse der BND-Amtsleitung und des Kanzleramtes bei der Fachaufsicht

Es ist kaum glaubhaft, dass im Zuge der *Snowden*-Enthüllungen weder Präsident *Schindler* noch das Kanzleramt beim BND nach der konkreten Praxis der Kooperation mit der NSA gefragt haben sollen. Dass der BND Suchbegriffe der NSA steuert, war allen Seiten bekannt. Die Frage, mit welchen NSA-Suchbegriffen der BND Telekommunikation erfasst, drängte sich bei den nahezu wöchentlichen Veröffentlichungen aus den *Snowden*-Dokumenten auf.

Präsident *Schindler* räumte vor dem Ausschuss sogar ein, dass es in den Gesprächen mit Kanzleramtsminister *Pofalla* im Sommer 2013 auch um NSA-Selektoren ging:

> „Es ging um die Problematik NSA. Und bei der Problematik NSA ging es auch darum: Wie läuft das Verfahren? Wenn Sie mitkriegen: „Wir steuern in Bad Aibling US-amerikanische Selektoren“, dann fragt man sich natürlich: „Wie läuft das Verfahren?“, und, und, und. Also, ich weiß, worauf Sie hinauswollen. Es ging auch immer mal um Selektoren, aber nicht um die 40 000er-Liste; die ist ja erst viel später ausgedruckt worden. Zum damaligen Zeitpunkt wussten wir gar nicht, dass eine solche 40 000er-Liste in der Maschine existierte.“[611]

---

610) Bundesregierung: Pressemitteilung Nr. 153 vom 23. April 2015, „Fernmeldeaufklärung des Bundesnachrichtendienstes“, https://www.bundesregierung.de/Content/DE/Pressemitteilungen/BPA/2015/04/2015-04-23-bnd.html, abgerufen am 6. Juni 2017.

611) *Schindler*, Protokoll-Nr. 126 I, S. 51.

Ob *Schindler* damals von der „40.000er-Liste“ als solche wusste, ist völlig unerheblich. Es wäre seine Pflicht gewesen, in der Abteilung TA nachzufragen, welche Selektoren der BND für die NSA steuert. Im Zusammenhang mit den BND-eigenen Selektoren hat Schindler sich diese Frage schließlich sehr wohl gestellt: Nach der Presseberichterstattung zum abgehörten Kanzlerinnen-Handy Ende Oktober 2013 und den erneuten Äußerungen *Merkels* („Abhören unter Freuden, das geht gar nicht“), gab Schindler den Auftrag an die Abteilung TA, ihm aufzulisten, welche Botschaften aus EU- und NATO-Staaten der BND steuert.[612] (Zu den unzulässigen BND-Selektoren siehe Kapitel VIII.)

Für das Kanzleramt gilt dies in gleicher Weise. Wenn es keine derartigen Nachfragen zur Kooperation mit der NSA, insbesondere zu den eingesetzten Suchbegriffen gegeben hat, wäre dies ein Versäumnis der Fachaufsicht durch BND-Amtsleitung und Kanzleramt. Anlasse zum Nachfragen gab es wegen der Snowden-Berichterstattung reichlich. Der Selektoren-Skandal und das Ausspionieren europäischer Nachbarstaaten durch die NSA mithilfe des BND wären womöglich noch vor der Wahl 2013 aufgedeckt worden.

d) Verschleppung des NSA-Selektoren-Problems bis März 2015 als Folge der Vertuschung

Das Verschweigen und Vertuschen des NSA-Selektorenproblems hatte weitreichende Folgen. Denn es ging soweit, dass nicht einmal der für die wöchentliche Selektorenprüfung zuständige BND-Mitarbeiter in Pullach, *K. M.*, von den Deaktivierungen in Bad Aibling und den Kriterien dafür erfahren hat. In seinem Zuständigkeitsbereich lagen die Filter und Wortbanken, mit denen die wöchentlich neu gelieferten NSA-Selektoren automatisiert geprüft wurden. Aber auch für die Pflege der Filter, mit denen die an die NSA zu übermittelnden Daten gefiltert wurden, war er zuständig.

Vor dem Ausschuss gab *K. M.* an, dass er von den Tausenden im Sommer 2013 aussortierten E-Mail-Adressen erst nach März 2015 erfahren habe.[613] Er habe weder von der Prüfung durch *Dr. M. T.* noch von den Deaktivierungen durch *W. O.* in Bad Aibling

612) Vgl. E-Mail des Stabsreferats TAZ vom 28. Oktober 2013, Betreff: Gesteuerte Vertretungen, MAT A BND-44/2 (Tgb.-Nr. 223/16 – GEHEIM), Ordner 432, Bl. 148 (VS-NfD).

613) *K. M.*, Protokoll-Nr. 62 I, S. 51.

gewusst.[614] Er kritisierte, dass es ihm daher nicht möglich gewesen war, die Prüfkriterien für die Filter anzupassen.[615]

K. M.s Arbeitsbereich hätte in jedem Fall umgehend von den Funden unzulässiger NSA-Selektoren informiert werden müssen, um die Filterkriterien anzupassen. Alle seine Vorgesetzte – der Unterabteilungsleiter *D. B.*, der Referatsleiter *H. K.* und auch sein direkter Vorgesetzter *T. B.* – wussten von dem Selektorenproblem. Aber sie schwiegen pflichtwidrig und gaben pflichtwidrig keine Anweisung, die Filter entsprechend anzupassen.[616]

Der Zeuge *D. B.* gab an, das Selektorenproblem vermeintlich dadurch für die Zukunft „gelöst“ zu haben, dass er den Dienststellenleiter von Bad Aibling, *R. U.*, noch im August 2013 beauftragt hatte, zum NSA-Verbindungsbüro SUSLAG in Bad Aibling zu gehen, und die NSA aufzufordern, „dieses zukünftig zu unterlassen bzw. selber aus der Erfassung zu nehmen“.[617]

Das ist an sich schon völlig unzureichend. Ein Vertrauen in die NSA, sich künftig aufgrund einer bloßen mündlichen Aufforderung an Vereinbarungen zu halten, ist nicht gerechtfertigt und erscheint angesichts der Schwere des Verstoßes und Vertrauensbruchs geradezu naiv.

R. U. selbst erwähnte übrigens nichts von einem solchen Gespräch mit SUSLAG; er hat ausgesagt, dass er nur mit seinem Mitarbeiter *W. O.* über das NSA-Selektoren-Problem gesprochen habe und ihn anwies, die Selektoren zu deaktivieren.[618]

Nach Unterlagen zur BND-internen Aufarbeitung der NSA-Selektoren-Problematik nach März 2015 habe es mehrere solcher Gespräche mit SUSLAG gegeben; die NSA-Verbindungsstelle habe sich aber nicht zuständig gesehen. Gespräche zwischen BND und zuständiger Ebene der NSA seien mehrmals verschoben worden. Erst im November 2014 fand schließlich ein Treffen mit verantwortlichen NSA-Vetretern statt, bei dem

---

614) *K. M.*, Protokoll-Nr. 62 I, S. 34.

615) *K. M.*, Protokoll-Nr. 62 I, S. 51.

616) Der Zeuge *D. B.* berief sich zu dieser Frage auf sein Auskunftsverweigerungsrecht, *D. B.*, Protokoll-Nr. 48 I, S. 127.

617) *D. B.*, Protokoll-Nr. 62 I, S. 93.

618) *R. U.*, Protokoll-Nr. 47 I, S. 17.

– wie von *D. B.* im August 2013 angewiesen – der NSA verdeutlicht wurde, dass solche Selektoren zum Ausspionieren europäischer Nachbarstaaten nicht gesteuert werden dürften.[619] Und auch bei diesem Gespräch konnte keine zeitnahe Lösung des NSA-Selektorenproblems erreicht werden.

Vor diesem Hintergrund konnte Unterabteilungsleiter *D. B.* im August 2013 keineswegs davon ausgehen, dass das Problem nun gelöst sei und neue, abgewandelte unzulässige EU-bezogene Selektoren von der NSA nicht mehr übermittelt würden. Die Kriterien für die wöchentliche Prüfung neuer NSA-Selektoren in der Zentrale waren nicht angepasst worden und in Bad Aibling fand unserer Kenntnis nach vor März 2015 keine weitere Selektorenprüfung statt. Die Prüfung im Sommer 2013 blieb – soweit der Ausschuss feststellen konnte – eine einmalige Angelegenheit.

Die Filterkriterien wurden erst ab März/April 2015 – letztlich als Folge des Ausschusses – modifiziert und erst damit wurde ein wirkliches dreistufiges Prüfverfahren für die NSA-Selektoren etabliert. Unlesbare Selektoren und Deutungen konnten damit jedoch weiterhin nicht überprüft werden.

Wegen der Vertuschung des Selektoren-Skandals hat die Fachaufsicht die Notbremse viel zu spät gezogen. Erst im Mai 2015 hat der Chef des Kanzleramtes, *Peter Altmaier*, angewiesen, dass keine NSA-Selektoren mehr gesteuert werden dürfen, deren Begründung der BND nicht nachvollziehen könne. Da die NSA dies nicht umsetzen konnte oder wollte, wurde bis auf Weiteres die Erfassung von Internetverkehren mit Selektoren in Bad Aibling eingestellt.[620] Diese Entscheidung war richtig und überfällig. Zu bezweifeln ist jedoch, dass sie ausreichend war. Auch die Überprüfbarkeit von Telefonie-Selektoren der NSA, die weiterhin eingesetzt werden, wirft nach wie vor rechtliche und praktische Fragen auf, die nicht gelöst sind. Es besteht daher die Gefahr des fortwährenden Rechtsbruchs.

619) Vgl. Vorhalt aus MAT A BND-73, Ordner 535, PDF-Seite 20, in: Protokoll-Nr. 126 II (Tgb.-Nr. 53/17 – STRENG GEHEIM, nur zur Einsicht in der Geheimschutzstelle des Deutschen Bundestages), S. 111 f.

620) *Süddeutsche.de* vom 6. Mai 2015, „BND stoppt Internet-Überwachung für NSA“, http://www.sueddeutsche.de/politik/geheimdienst-affaere-bnd-stoppt-internet-ueberwachung-fuer-die-nsa-1.2468701.

e) Offene Fragen und schwarze Löcher

Wie oben dargestellt wurde dem Ausschuss von der Bundesregierung die Einsicht in die im August 2013 vom BND aussortierten NSA-Selektoren verweigert; ebenso der BfDI, der G 10-Kommission und dem Parlamentarischen Kontrollgremium. Den Gesamtbestand aller gelieferten Selektoren, d. h. der aktiven, der aussortierten (auf „disapproved“ gesetzten) und von der NSA auf inaktiv gesetzten, zurückgezogenen Selektoren, hat sich auch nicht die „Sachverständige Vertrauensperson“ der Bundesregierung, *Graulich*, angesehen.

Der Gesamtbestand der NSA-Selektoren hat sich zwischen August 2013 und März 2015 fast verdoppelt. Es gibt also eine riesige Anzahl „neuer“ NSA-Selektoren, die zwischen 2013 und dem Aufdecken des Skandals im Frühjahr 2015 offenbar nicht anhand des modifizierten Filters überprüft wurden. Und gar nicht überprüft werden konnten, da in dem Filtersytem in der BND-Zentrale solche Kriterien zur Erkennung staatlicher Stellen von EU- und NATO-Staaten erst Mitte März 2015 implementiert wurden. Wenn die veröffentlichten Angaben stimmen, handelt es sich um 7 bis 8 Millionen unzureichend geprüfter NSA-Selektoren. Angesichts der Selektorenzunahme erscheint auch fraglich, inwieweit die NSA unzulässige Selektoren, wie von BND-Zeugen behauptet, „zurückgezogen“ hat. Es sieht vielmehr danach aus, dass andere, neue Selektoren geliefert wurden.

Welche Ziele mit diesen Selektoren erfasst werden sollten, müssten mittlerweile BND und Kanzleramt wissen, sofern die Selektoren „lesbar“ oder zuordenbar waren. Denn nach der Aufdeckung im März 2015 fanden umfangreiche Suchläufe über den Selektorenbestand und Bereinigungen statt. Auch inwiefern diese Selektoren tatsächlich verwendet wurden oder nur „inaktiv“ in der Datenbank schlummerten, muss dort bekannt sein.

Dies alles konnte der Ausschuss nicht untersuchen. Zum einen gab es einen Streit über die Auslegung des erweiterten Untersuchungsauftrages hinsichtlich der NSA-Selektorenproblematik.[621] Die Koalition schlug sich erwartungsgemäß auf die Seite der

621) siehe Ziffer Ia Nr. 5 im erweiterten Auftrag, Bundestagsdrucksache 18/8683 vom 6. Juni 2016.

Bundesregierung und wollte hierzu anscheinend keine Aufklärung. Zum anderen verweigert die Bundesregierung weiterhin generell Angaben über die Inhalte der NSA-Selektoren.

Zu einem Abwiegeln hinsichtlich des Umfangs der im August 2013 beanstandeten NSA-Selektoren oder möglicher Wirtschaftsspionage, wie *Graulich* und die Koalition es tun, besteht daher insgesamt kein Anlass. Im Gegenteil: Es steht vielmehr zu befürchten, dass die Verstöße noch viel gravierender sind, als zum Zeitpunkt März 2015 bekannt war.

Um valide Aussagen treffen zu können, hätte man den Gesamtbestand der NSA-Selektoren untersuchen müssen, wie wir immer wieder gefordert haben. Welche Bewertungen wir bei Durchsicht aller NSA-Selektoren getroffen hätten, muss offen bleiben.

9. Datenübermittlungen des BND an die NSA aus Bad Aibling

„Massenerfassung – dafür können Sie Internetkabel nehmen“, verkündete ein ehemaliger BND-Mitarbeiter vor dem Untersuchungsausschuss. Und um „die Abteilung 2 [des BND] mit Gerät zu befähigen, dass sie ins Internet über Kabel eindringen kann“, sowie zur „Bewältigung von Massenerfassung“ wurde so ein Gerät auf die „Wunschliste“ für technische Systeme und Softwareroutinen bei der NSA gesetzt.[622] Der Deal war somit komplett: Technik gegen Daten – massenhaft Daten. So verlief die Operation EIKONAL; sie war ein – nach Unterlagen von *Edward Snowden* – für die NSA typisches Kooperationsmodell mit anderen Nachrichtendiensten: sie war ein Tauschgeschäft. Die NSA lieferte dem BND die begehrte Überwachungstechnik in Form von Hard- und Software und erhielt im Gegenzug den Zugriff auf damit gewonnene Daten. Diese erfasste der BND in der Operation EIKONAL aus deutschen Glasfasernetzen, bei einem deutschen Netzbetreiber, vermutlich auch aus Kabelabgriffen im außereu-

622) *Breitfelder*, Protokoll-Nr. 28 I, S. 25; MAT A BND-8a, Bl. 21-27 (VS-NfD).

ropäischen Ausland (Operation [redacted], oder aktuell aus der gemeinsamen Satellitenerfassung in Bad Aibling.[623] Insbesondere Bad Aibling gilt für die Kooperation des BND mit der NSA als zentrale Schnittstelle. Daneben, so ein *Snowden*-Dokument, soll die NSA auch Daten aus der Erfassung in der Außensstelle Schöningen erhalten haben.[624]

In welchem Umfang aus Bad Aibling Daten an die NSA übermittelt werden, wurde erst im Spätsommer 2013, im Zuge der *Snowden*-Enthüllungen, deutlich – war der BND doch zuvor äußerst bemüht, nur die Übermittlung von einigen ausgewählten „Meldungen" in den Fokus zu stellen. Tatsächlich erhielt die NSA jedoch nach Zeugenaussagen „sowohl Daten, die leitungsgebunden waren, es waren auch Daten paketvermittelter Art, und es waren auch Daten, die sich um die Kommunikationsumstände ranken, landläufig als Metadaten bezeichnet. Und es waren auch Daten, die entsprechend aufbereitet wurden, beispielsweise aus der Signalanalyse."[625] Die massenhafte Übermittlung von Metadaten wurde so lange verheimlicht und verharmlost.

Der BND unterscheidet fälschlicherweise bei der Eingriffsintensität hinsichtlich Inhalts- und Metadaten, um Letztere nicht nur im Zusammenhang mit Kommunikationsinhalten zu übermitteln, sondern sie massenhaft, als Datenströme ganzer Kommunikationsstrecken auszuleiten und automatisiert an die NSA weiterzugeben.

Unabhängig von der Art personenebezogener Daten stellt jedoch jede Form der Überwachung einen Eingriff in die Freiheitsrechte und Persönlichkeitsrechte der/s Überwachten dar.

Bereits die Datenabgriffe durch den BND, aber auch die anschließenden Speicherungen sind hier aufgrund der fehlenden Rechtsgrundlage und der Unverhältnismäßigkeit – insbesondere der Metadatenerfassung – aufgrund ihrer Massenhaftigkeit erhebliche

623) BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015, veröffentlicht auf netzpolitik.org, https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/, abgerufen am: 15. Juni 2017.

624) MAT A Sek-4/1q, „NSAers Make First-Ever Visit to FORNSAT Collection Site in Schöningen, Germany", http://www.spiegel.de/media/media-34099.pdf, abgerufen am 16. Juni 2017.

625) *T. B.*, Protokoll-Nr. 24 II – Auszug offen, S. 33; vgl. R. U., Protokoll-Nr. 47 I, S. 6.

Grundrechtsverstöße (Abschnitt V.9.a)aa)). Eine nachfolgende Weiterleitung der Daten und zum Teil sogar gemeinschaftlich vorgenommene Speicherung und Analyse in gemeinsamen Dateien war schon deshalb in rechtmäßiger Art und Weise nicht mehr möglich, da sie hätten gelöscht werden müssen. Diese Übermittlungen stellen jedoch selbst auch eigenständige, massive Grundrechtseingriffe dar, für die es ebenfalls an einer hinreichenden Rechtsgrundlage fehlte.

Diese Maßnahmen des BND waren auch deshalb rechtswidrig, da der BND die nach seiner Auffassung geltenden einfachgesetzlichen Vorgaben für die Übermittlungen von Metadaten (Abschnitt V.9.a)) und Inhaltsdaten (Abschnitt V.9.b)) an die NSA nicht einhielt.

Es handelt sich hierbei um klare und schwere Verstöße gegen die Freiheitsrechte einer Vielzahl völlig unbescholtener Personen. Die Massenüberwachung des BND ist hier als Gesamtprozess zu werten, er ist „datenschutzrelevant und relevant für das Fernmeldegeheimnis“.[626] Der Eingriff in den Schutzbereich des Art. 10 Abs. 1 GG[627] ist nicht auf die Erfassung der Daten begrenzt. Vielmehr stellt jede einzelne Verwendung, d. h. Speicherung, Veränderung, Übermittlung, Sperrung und Löschung oder Nutzung eines personenbezogenen Datums nach der Rechtsprechung des Bundesverfassungsgerichts einen rechtlich eigenständigen Grundrechtseingriff dar und ist daher von anderen Eingriffstatbeständen losgelöst zu bewerten.[628]

626) *Schaar*, Protokoll-Nr. 31 I, S. 28.

627) siehe hierzu Abschnitt V.3.b)bb) zum verfassungsrechtlichen Maßstab.

628) BVerfGE 100, 313, (359 und 366f.), http://www.bverfg.de/e/rs19990714_1bvr222694.html; BVerfGE 125, 260 (309 f.), http://www.bverfg.de/e/rs20100302_1bvr025608.html; *Papier*, Beschränkung der TK-Freiheit, NVwZ – Extra 15/2016, S. 1 (3), abrufbar unter http://rsw.beck.de/rsw/upload/NVwZ/NVwZ-Extra_2016_15.pdf; vgl. BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015, dort 1, A, II, 1, a), https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/

a) Rechtswidrige Ausleitung von Metadaten aus kompletten Strecken und Übermittlung an die NSA

aa) Umfang der Datenerfassung und Weitergabe an die NSA

> **Zeuge *T. B.*:** „Eine massenhafte Metadatenerfassung gab es noch nicht, weil wir mit den Metadaten im ersten Ansatz noch nichts anfangen konnten."

> **Vorsitzender Dr. *Patrick Sensburg*:** „Ab wann gab es denn die massenhafte Metadatenerfassung?"

> **Zeuge *T. B.*:** „Tut mir leid, weiß ich nicht."

> **Vorsitzender Dr. *Patrick Sensburg*:** „Okay, aber zumindest wissen wir schon mal, dass es sie gab."[629]

Aufgrund zwei weitere Jahre andauernder Zeugenbefragungen wissen wir noch mehr: Sicher ist, dass sich der BND nicht mehr darauf berufen kann, nichts von der enormen Bedeutung der Metadaten gewusst zu haben. Bereits um das Jahr 2000 hatte auch der BND bemerkt, „dass grundsätzlich auf der Welt das Internet beherrschend wird und man dazu neue Methoden braucht. Stichwort: Metadaten."[630] Vor diesem Hintergrund erklärten die NSA nach dem Motto „do ut des" den BND-Mitarbeiter_innen, „wir [können] euch schon das Laufen beibringen".[631] Für den BND war dies ein verlockendes Angebot: „Know-how und Technik und dazu noch ein paar kundige NSA-Mitarbeiter weiter dahaben, das könnte es doch sein. Es war schon klar, dass wir auch gerne irgendwo mal in der Welt ans Kabel müssten und dass auch diese Metadaten bei Erfassungen eine große Rolle spielen werden."[632]

---

629) *T. B.* und Vorsitzender *Dr. Patrick Sensburg*, Protokoll-Nr. 20 I, S. 14.

630) *Dr. Fechner*, Protokoll-Nr. 41 I, S. 15.

631) *Dr. Fechner*, Protokoll-Nr. 41 I, S. 16.

632) *Dr. Fechner*, Protokoll-Nr. 41 I, S. 16.

So lernten die BND-Mitarbeiter_innen von der NSA bereits „früher Massendaten aus dem Internet bewältigen und aufklären zu können.“[633] Auch der Zeuge *W. K.,* Leiter der Unterabteilung T1 im Bereich der Technischen Aufklärung, gab vor dem Untersuchungsausschuss an: „Natürlich haben Sie heutzutage immer Massendaten im Internet. […] Wir hatten die technische Fähigkeit, damit umzugehen.“[634] Der BND stellte große Teile seiner Maßnahmen auf die Auswertung von Metadaten um. In Folge dessen griff der BND nicht nur massenhaft und pauschal, d. h. anlasslos Metadaten ab, sondern leitete diese auch automatisiert und komplett, das heißt ohne vorherige inhaltliche Prüfung oder Auswahl und gleichfalls massenhaft an die NSA weiter. Die Metadaten sollten lediglich um die Daten von Deutschen (Personen oder Firmen) und sich in Deutschland aufhaltenden Personen bereinigt werden. Die Beweisaufnahme hat gezeigt, dass das dafür eingesetzte Filtersystem jedoch bereits vom Ansatz her unzureichend war (siehe hierzu unter V.6 – „Zu Risiken und Nebenwirkungen…“ sowie V.7 – „Ungelöste Filterproblematik“).

Dabei griff der BND in die Vertraulichkeit der näheren Umstände von Telekommunikationsvorgängen ein, die gleichwohl vom grundrechtlichen Schutz des Telekommunikationsgeheimnisses geschützt ist[635] und beging damit massenhaft schwerwiegende Grundrechtsverstöße. Für diesen Eingriff gibt es keine Rechtfertigungsgrundlage. Diese Praxis der Metadatenerfassung und -übermittlung stellt in ihrer Art als auch ihrem Umfang eine qualitativ wie quantitativ völlig neue Dimension der Überwachung durch Geheimdienste dar. Sie kann nicht mehr im Verhältnis zur bloßen Möglichkeit oder Nützlichkeit für eine eventuelle Gefahrenprävention stehen, geschweige zur bloßen Sammlung von außen- und sicherheitspolitischen Informationen zur Erkenntnisgewinnung. Vielmehr gleicht sie einer weitgehend anlasslosen Massenüberwachung und ist daher mit dem im Grundgesetz geforderten Grundsatz der Verhältnismäßigkeit nicht mehr vereinbar und daher rechtswidrig. Die Auswirkungen dieser Praxis sind und

633) *Süddeutsche Zeitung* vom 4. Oktober 2014, „Codewort Eikonal“; BND-interner Vermerk von Herrn *R.* an u. a. *Hanning*, vom 28. April 2008, vgl. Aktenvorhalt in Protokoll-Nr. 22 III – Auszug offen, S. 59 f.

634) *W. K.*, Protokoll-Nr. 22 III – Auszug offen, S. 55.

635) *Hans-Jürgen Papier*, Beschränkungen der Telekommunikationsfreiheit durch den BND an Datenaustauschpunkten, *NVwZ-Extra* 15/2016, S. 1 (3), abrufbar unter http://rsw.beck.de/rsw/upload/NVwZ/NVwZ-Extra_2016_15.pdf.

bleiben enorm, gerade im Hinblick auf die wachsende Bedeutung der Metadaten und der Möglichkeiten ihrer Verwendungen.

aaa) Massenüberwachung

Im Sommer 2013 berichtete *Der Spiegel* unter Berufung auf eine von *Edward Snowden* an Journalist_innen übergebene Statistik des NSA-Programms BOUNDLESS INFORMANT, dass die NSA allein im Dezember 2012 aus Deutschland rund 500 Millionen Kommunikationsverbindungsdaten, darunter von Telefonaten, E-Mails, SMS oder Chatbeiträgen, aus der Fernmeldeaufklärung/Satellitenerfassung erfasst habe. „Gespeichert werden diese Metadaten anschließend im Hauptquartier der Behörde in Fort Mead, nahe Washington“.[636] Nach den Veröffentlichungen der Zahlen begann der BND intern selbst zu recherchieren. Zwar konnten Bundesregierung und BND mit Hilfestellung der NSA den Verdacht vorerst abbiegen, die NSA würde selbst Metadaten in dieser Höhe aus Deutschland von Deutschen erheben. Sie präsentierten der Öffentlichkeit als Erklärung, dass die in der veröffentlichten Statistik erwähnten und bei der NSA unter der Kategorie „Most Volume“ laufenden SIGINT-Quellen (SIGAD) US-987LA und US-987LB den Erfassungsstellen des BND in Bad Aibling und in Afghanistan zuzuordnen seien.[637]

Tatsächliche Belege gibt es dafür nicht, lediglich Versicherungen der US-Seite, um die die Bundesregierung geradezu bettelte. Jedoch konnte nach der *Spiegel*-Veröffentlichung nicht mehr geleugnet werden, dass der BND selbst in einem bis dahin nicht öffentlich gekannten Ausmaß massenhaft Kommunikationsverbindungsdaten erhebt und an die NSA übermittelt.

---

636) *Der Spiegel* vom 29. Juli 2013, „Tricks und Finten“; BOUNDLESS INFORMANT, Germany – Last 30 days, http://www.spiegel.de/media/media-34055.pdf, abgerufen am 17. Juni 2017; *Glenn Greenwald*, Die Globale Überwachung, 2014, S. 148; *R. U.*, Protokoll-Nr. 14 I, S. 33.

637) Pressestatement von Kanzleramtsminister *Pofalla* nach der Sitzung des Parlamentarischen Kontrollgremiums am 12. August 2013, https://www.bundesregierung.de/ContentArchiv/DE/Archiv17/Mitschrift/Pressekonferenzen/2013/08/2013-08-12-pofalla.html, abgerufen am 5. Juni 2017; Antwort der Bundesregierung auf die Kleine Anfrage der SPD, Bundestagsdrucksache 17/14560 vom 14. August 2013, S. 8, http://dipbt.bundestag.de/doc/btd/17/145/1714560.pdf, abgerufen am 17. Juni 2017.

Dabei soll es sich nicht um einzelne Metadaten handeln, sondern um Metadatensätze. Der Umfang der erfassten und weitergeleiteten Daten ist daher im Ergebnis noch deutlich umfangreicher. Auch handelt es sich bei der BOUNDLESS INFORMANT-Statisitk um eine Darstellung für einen Zeitraum von lediglich dreißig Tagen. „Die Zahlen schwanken“, so der BND.[638]

Aus den Akten ziehen wir den Schluss, dass sich der BND sogar bemühen musste, bei den daraufhin veranlassten Zählungen die Summe von ca. 580 Millionen Datensätzen darstellen zu können; tatsächlich war die Anzahl der an die NSA übermittelten Metadaten – ohne dass wir hier genauer werden dürfen – deutlich größer.[639] BND-intern wurde gegenüber der behördlichen Datenschutzbeauftragten am 20. August 2013 bestätigt, dass eine Datenweitergabe im Umfang von ca. 1,3 Milliarden Daten pro Monat erfolge.[640] BND-Mitarbeiter_innen bestätigten vor dem Untersuchungsausschuss diesen Umfang.[641] „Die Zahlen sprechen für sich“[642], resümmierte die Zeugin *Löwnau* von der BfDI.

D. B., Unterabteilungsleiter T2 der Technischen Aufklärung, hat gegenüber der Datenschutzbeauftragten des BND, *Dr. H. F.* auf Nachfrage eingeräumt, „dass die vorgenannte Weitergabe von Rohdaten [aus Bad Aibling] an US-SUSLAG [die Verbindungsstelle der NSA] in großem Umfang stattfinde. Es würden auf bestimmten Übertragungswegen im Ausland alle durch den BND erhobenen Daten an US-SUSLAG weitergegeben.“[643]

Im Untersuchungsausschuss wurde noch einmal besonders deutlich, beim Thema Massenüberwachung „geht [es] nicht um die Frage: Ab soundso viel Millionen oder,

---

638) *W. K.*, Protokoll-Nr. 22 III – Auszug offen, S. 45.

639) Siehe MAT A BND-8b (Tgb.-Nr. 54/14 – GEHEIM), Ordner 198, Bl. 69-70, 73-75; MAT A BND-54 (Tgb.-Nr. 235/16 – GEHEIM), Ordner 457, Bl. 7-12; MAT A BND-1/14f (Tgb.-Nr. 110/15 – GEHEIM) Anl. 03, Ordner 311, Bl. 218-227.

640) Vermerk der BND-Datenschutzbeauftragten H. F. v. 20. August 2013, MAT A BND-1/6a, Bl. 239 (VS-NfD), Aktenvorhalt in Vernehmung *Pauland*, Protokoll-Nr. 50 I, S. 60.

641) *Breitfelder*, Protokoll-Nr. 50 I, S. 60; *Pauland*, Protokoll-Nr. 50 I, S. 203.

642) *Löwnau*, Protokoll-Nr. 72 I, S. 60.

643) Vermerk der BND-Datenschutzbeauftragten H. F. v. 20. August 2013, MAT A BND-1/6a, Bl. 239 (VS-NfD); Aktenvorhalt in Vernehmung *R. U.*, Protokoll-Nr. 47 I, S. 21.

was weiß ich, Tausend oder wie auch immer Daten spreche ich von einer Massendatenerfassung, sondern ich kann eigentlich in jeder Quantität von Massendatenerfassungen sprechen, wenn denn entsprechend der Prozess unterschiedslos und automatisiert abläuft.“[644] Vorliegend ist dies nicht nur für die Datenerfassung, sondern auch für ihre Übermittlung durch den BND nachgewiesen.

bbb) Unterschiedslose Erfassung

Herr *Alster* von der *Telekom* erklärte vor dem Untersuchungsausschuss: „Also, wenn Sie mich jetzt fragen würden: „Was wird abgehört in Russland?“, würde ich sagen: Alles.“[645] Nach Auffassung von Bundesregierung und BND ist die Massendatenerfassung hingegen nicht unterschiedslos, da:

„[redacted].“[646]

Die Auswahl traf der BND also vor der Ausleitung und Datenübermittlung nicht durch eine vorherige Selektion, sondern lediglich durch die Streckenauswahl der Auslands-Auslands-Übertragungswege nach nachrichtendienstlichen Gesichtspunkten und dem Auftragsprofil der Bunderegierung:[647] „Aufgrund der Streckenbeziehungen wissen Sie, von wo nach wo diese Strecke geht. Das heißt auch, Sie können abschätzen, welche Nutzer darauf sind.“[648] Im Ergebnis stellt dies keine hinreichende Auswahl dar. Unter anderem unterliegt die Beschaffenheit von Datenströmen – also welche Daten aus welchen Regionen transportiert werden – ohnehin erheblichen Schwankungen. Sie

---

644) Abgeordneter *Flisek*, Zusammenfassung der Aussage von *Schaar*, Protokoll-Nr. 31 I, S. 24.

645) *Alster*, Protokoll-Nr. 30 II – Auszug offen, S. 20.

646) Bundeskanzleramt, Referat 601, Ergebnisprotokoll, Vorbesprechung des Kontrollbesuchs des BfDI in Bad Aibling am 2. und 3. Dezember 2013, MAT A BK-1/6b, Bl. 292 f. (293).

647) Vgl. E-Mail von *A. F.* an *Dr. H. F.* vom 21. August 2013, MAT A BND-40a, Bl. 139 f. (139) (VS-NfD).

648) *T. B.*, Protokoll-Nr. 24 II – Auszug offen, S. 54.

ändern sich immer, wenn der Betreiber neue Strecken auflegt. Es handelt sich hierbei also lediglich um eine Prognose, die insbesondere aufgrund der Beschaffenheit moderner digitaler Leitungswege und der Technik im Zeitalter der Globalisierung äußerst grob und fehlerhaft ist.

Für die Übermittlung von Metadaten aus IP-Verkehren im Rahmen Operation EIKONAL an einem Frankfurter Kabelknoten stellte sich dies in gleicher Weise dar. Auch dort wurden Metadaten unabhängig von Suchbegriffen oder Selektoren aus den ausgewählten Strecken an die JSA weitergeleitet und standen – nach dem sie einen „G 10-Filter“ durchlaufen hatten – der NSA zur Verfügung.

bb) Metadaten besitzen eine hohe Aussagekraft

Es ist – abseits des Profits des BND – nicht erkennbar, weshalb Inhaltsdaten und Metadaten getrennt voneinander unterschiedliche Behandlung erfahren sollen. Das *BVerfG* verdeutlichte in seiner Rechtsprechung, dass Verkehrsdaten eine weitreichende Aussagekraft besitzen.[649]

Welches Verständnis über Metadaten im BND vorherrscht, beschreibt der Zeuge Pauland vor dem Untersuchungsausschuss wie folgt:

> „Wir verstehen im Dienst unter den Metadaten Sach- und Verkehrsdaten, also alle Daten, die das Umfeld einer Kommunikation beschreiben, die anfallen auf der technischen Seite beim Umfeld einer Kommunikation. Das heißt, es kann natürlich eine E-Mail-Adresse sein, es kann natürlich eine Telefonnummer sein, aber es kann auch die Einstellung Ihres Browsers sein. Es kann sein: Welche Sprache hat der Browser? – So hinterlässt jeder seine Spuren oder jeder hat ein Profil auf seinem Rechner, weil jeder sich ja selbst heutzutage alles einstellen kann. Und da gibt es eben eine Unzahl, Vielzahl von Metadaten.“[650]

649) BVerfGE 125, 260 (319), http://www.bverfg.de/e/rs20100302_1bvr025608.html.

650) *Pauland*, Protokoll-Nr. 50 I, S. 15.

Für den BND sind die Metadaten genauso wichtig wie der Inhalt einer Unterhaltung, wenn nicht gar wichtiger, denn sie können sogar weitaus aussagekräftiger als konkrete Kommunikations-Inhalte sein. Die Datenschutzbeauftragte des BND bestätigte, dass die Metadaten für die Nachrichtendienste „interessant geworden sind (…), weil man erkannt hat, dass man durch diese Auswertungen viele Erkenntnisse bekommen kann und dass das eben von Interesse ist auch für Beziehungsdarstellung usw.“[651] Es lassen sich Beziehungsgeflechte darstellen und genau analysieren. So kann der BND verfolgen, wer zu welchem Zeitpunkt, an welchem Ort und mit welchen Personen, auf welche Art und Weise kommuniziert. Mittels Metadaten lassen sich so auch verlorengegangene Ziele (Targets) wiederfinden, wenn sie mit neuen Kommunikationsmitteln kommunizieren.[652]

Diese massenhaften Metadaten werden von den Nachrichtendiensten permanent durchsucht und gerastert – vornehmlich um nachrichtendienstlich relevante Personen aufzufinden. „Von mittelbarer ND-Relevanz sind alle Personen, die zu einer unmittelbar ND-relevanten Person in einer Beziehung stehen oder wenn Metadaten aufgrund einer geographischen Betrachtungsweise gespeichert werden. Der Bezug zur unmittelbar ND-relevanten Person kann über beliebig viele Ebenen erfolgen. *VERAS 6* enthält keine Zuordnungsbegrenzung,“[653] stellte die BfDI fest. Auch die BND-Datenschutzbeauftragte *Dr. H. F.* bestätigte, dass der BND hierbei Zugriff auf sämtliche Verbindungsdaten hat und diese nutzt, um ungebremst in alle Verbindungsebenen von Kontaktpersonen vorzudringen. Denn es „gibt keine festen Ebenen; das System selber bremst einen auch nicht aus, wenn man in die siebte oder achte Ebene gehen würde.“[654]

Darüber hinaus können „[i]n Kombination mit den (…) technischen Möglichkeiten, (…) nicht nur diese Verbindungsebenen beliebig erweitert und technische Selektionen

---

651) *Löwnau*, Protokoll-Nr. 72 I, S. 136.

652) Vgl. *R. U.*, Protokoll-Nr. 14 II – Auszug offen, S. 32.

653) BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015, 1, A, I, 1, a, aa), https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/.

654) *H. F.*, Protokoll-Nr. 121 I, S. 9.

durchgeführt sowie bestimmte Personen gezielt fokussiert, sondern auch Bewegungsprofile dieser Personen erstellt werden.“[655]

Darüber hinaus spielt der metadatenzentrierte Ansatz eine große Bedeutung in der Geheimdienstpraxis. Eine Inhalts-Erfassung bedarf nunmehr keiner Suche mit feststehenden Selektoren mehr, sondern kann mittels Metadaten erfolgen. Hierfür werden bestimmte darin enthaltene Muster zusammengeführt.

Metadaten geben tiefe Einblicke in das soziale Umfeld von Betroffenen frei und lassen Rückschlüsse auf ihre individuellen Aktivitäten zu. Die in ihnen enthaltenen Informationen lassen Verhaltensmuster erkennen und ermöglichen unter anderem die Darstellung von Bewegungsprofilen und sozialen Beziehungsgeflechten. Interpretationen dieser Daten ermöglichen auch Vorhersagen darüber, was eine bestimmte Person als Nächstes tun wird, oder wo sie sich zu einem bestimmten Zeitpunkt aufhalten wird. Mit ihrer Hilfe lassen sich jedoch auch soziale Graphen ganzer Gesellschaften erstellen.[656]

Der BND leitete die Daten in massenhaftem Umfang an die NSA weiter, mit dem Bewusstsein über ihre weiten Verarbeitungs- und Analysemöglichkeiten, aber auch mit der fehlenden Kenntnis über ihre tatsächliche Verwendung. So erklärte der Zeuge Breitfelder vor dem Untersuchungsausschuss, dass „diese Daten, zum Beispiel Routingdaten von Netzwerken und so was, (…) an die NSA [gingen] und die hat damit Netzwerke analysiert und, ja, vielleicht genutzt, um andere Ansätze zu optimieren – keine Ahnung. Das war die Sache mit den Metadaten.“[657] Doch der frühere NSA- und CIA-Chef *Michael Hayden* formulierte bei einem Podium in der John-Hopkins-Universität Baltimore am 1. April 2014 die Bedeutung für Arbeit der NSA öffentlich und sehr klar: „We kill people based on metadata.“[658]

655) BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015, 1, A, I, 1, a, aa), https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/.

656) Deutscher Bundestag, Wissenschaftlicher Dienst, Ausarbeitung „Verfassungsfragen des Entwurfs eines Gesetzes zur Ausland-Ausland-Fernmeldeaufklärung des Bundesnachrichtendienstes“, WD 3 – 3000 – 194/16, S. 12.

657) *Breitfelder*, Protokoll-Nr. 28 I, S. 66

658) Video abrufbar unter https://www.youtube.com/watch?v=kV2HDM86XgI, ab Minute 18:00.

cc) Rechtswidrigkeit aufgrund fehlender Dateianordnungen

Aufgrund fehlender Dateianordnungen ist bereits die Datenerfassung rechtswidrig. Sämtliche daran anschließenden Verwendungen und Übermittlungen sind folglich allein deshalb schon rechtswidrig.

Gemäß § 6 S. 1 BNDG ist der BND ausdrücklich dazu verpflichtet, über jede automatisierte Datei mit personenbezogenen Daten eine Dateianordnung nach § 14 BVerfSchG zu führen und hierin unter anderem den Zweck und die Art der Datenerhebungen sowie Voraussetzungen der Speicherung, Übermittlung und Nutzung zu definieren (§ 14 Abs. 1 S. 1 Nr. 2, 3 BVerfSchG). Bei Dateianordnungen handelt es sich um „relativ umfängliche, detaillierte Beschreibungen, was Sinn und Zweck der Datenbank ist, wer Zugriff haben soll, in welchem Umfang er Zugriff haben soll, welche Personen gespeichert werden sollen, wie die Technik ist, was für eine Datenbanktechnik dahinter liegt. Es bedarf also einer sehr intensiven Abstimmung mit dem Bedarfsträger.“[659] Sinn und Zweck solch „verfahrenstechnischer und verfahrensrechtlicher Schranken“ ist die Sicherstellung, „daß die gespeicherten personenbezogenen Daten nicht über das für die Aufgabenerfüllung erforderliche Maß verwendet, weitergegeben oder aufbewahrt werden“.[660]

Der BND jedoch hielt sich nicht an diese gesetzliche Vorschrift. Er errichtete und verwendete mindestens sieben automatisierte Dateien i. S. v. § 11 BNDG i. V. m. § 46 Abs. 1 Nr. 1 BDSG ohne eine solche Anordnung. Dies betraf in Bad Aibling die Dateien VERAS 4, VERAS 6, XKEYSCORE, TND, SCRABBLE, INBE und DAFIS. Hierbei handelt es sich um Dateien, die der BND nutzte, um unter anderem in großem Umfang personenbezogene Metadaten zu gewinnen, zu speichern und zu verwenden, d. h. durch automatisierte Verfahren nach bestimmten Merkmalen auszuwerten.[661] Weiterhin holte der BND weder die notwendige Zustimmung des Kanzleramtes ein (§ 6 S. 1

---

659) *H. F.*, Protokoll-Nr. 16 I, S. 32; Bedarfsträger sind z. B. die Bereiche des BND, in denen die Auswertung der Daten zu bestimmten Themengebieten stattfindet.

660) Gesetzentwurf der Bundesregierung. Entwurf eines Gesetzes zur Fortentwicklung der Datenverarbeitung und des Datenschutzes, Bundestagsdrucksache 11/4306, S. 62.

661) Vgl. *Löwnau*, Protokoll-Nr. 72 I, S. 136.

BNDG), noch kam er der nach § 6 S. 1 BNDG i. V. m. § 14 Abs. 1 S. 2 BVerfSchG. vorgeschriebenen vorherigen Anhörungspflicht durch die BfDI nach.

Diese externen Vorabkontrollen stellen jedoch eine zentrale Schutzfunktion, im Hinblick auf die Wahrung der Grundrechte von Betroffenen, dar. Dies gilt insbesondere, da es sich vorliegend um heimliche Grundrechtseingriffe handelt, die einer besonderen Kontrolle bedürfen. Die BfDI sah darin schwerwiegende Rechtsverstöße und beanstandete sie gemäß § 25 Abs. 1 S. 1 BDSG.[662]

Zahlreiche Datenbanken erfüllten somit weder die formellen, noch die materiellen rechtlichen Erfordernisse, die für das Betreiben solcher Datenbanken unerlässlich wären.[663] Der BND konnte oder wollte nicht sicherstellen, dass die gespeicherten Daten nicht über das für seine Aufgabenerfüllung erforderliche Maß hinaus verwendet werden. Eine rechtskonforme Verwendung der erhobenen Informationen konnte unter diesen Umständen gar nicht mehr erfolgen.

Dennoch wurden, so bemängelte die BfDI, die „Daten ohne die in den jeweiligen Dateianordnungen festzulegenden Vorgaben – insbesondere die Festlegung des konkreten Zwecks der Datei – verwendet".[664] Bei diesen Zweckbegrenzungen handelt es sich jedoch gerade um „zentrale verfassungsgerichtlich geforderte Begrenzungen für die aus den Verwendungen dieser Daten resultierenden Grundrechtseingriffe".[665] Ohne diese Festschreibung wurden die Dateien sogar über Jahre hinweg verwendet.[666] Die Mitarbeiter_innen des BND wurden in Folge der Beanstandungen durch die BfDI aufgefordert, jede weitere Verwendung der hierin enthaltenen Daten zu unterlassen und die gespeicherten Dateien unverzüglich zu löschen (§ 5 Abs.1 BNDG i. V. m. § 12 Abs.

662) BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015, 1, A, II, 1 u. 3), https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/; vgl. *Löwnau*, Protokoll-Nr. 72 I, S. 42 ff.; vgl. H. F., Protokoll-Nr. 16 I, S. 38.

663) BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015, 1, A, II, 2, a), https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/; *Löwnau*, Protokoll-Nr. 72 I, S. 62 f.

664) BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015, 1, A, II), https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/.

665) BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015, 1, A, II, 2, a), https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/.

666) *H. F.*, Protokoll-Nr. 16 I, S. 32.

2 S. 1 BVerfSchG). Zudem wurde der BND verpflichtet für u. a. die Programme *SCRABBLE*, *TND* und *XKEYSCORE* entsprechende Dateianordnungsentwürfe zu erstellen und vorzulegen.[667]

Nicht nur jede Erhebung, auch jede einzelne Verarbeitung, jede einzelne Übermittlung eines betroffenen personenbezogenen Datums an die NSA ist folglich formell und materiell rechtwidrig geschehen und stellt für sich gesehen jeweils einen eigenen Eingriffstatbestand dar.

dd) Automatisierte Übermittlung massenhafter Metadaten an die NSA

Jede Datenübermittlung des BND an die NSA ist ein Eingriff in das Telekommunikationsgeheimnis gemäß Art. 10 GG sowie das Grundrecht auf informationelle Selbstbestimmung.

Datenübermittlungen personenbezogener Daten, die der BND für seine legitimen Zwecke aus der Telekommunikationsüberwachung erlangt hat, an ausländische öffentliche Stellen können zwar in Einzelfällen, in gewissem Umfang und unter Beachtung der gesetzlichen Vorgaben mit Art. 10 GG vereinbar sein.[668] Bei der Datenweiterleitung des BND an die NSA in Bad Aibling ging es jedoch nie um Einzelfälle. Der BND übermittelte die Metadaten ebenfalls massenhaft und automatisiert an die NSA, indem er sie als Datenstrom, das heißt unbearbeitetes Datenmaterial – ausschließlich automatisiert „G 10-gefiltert“ – aus ganzen Strecken ausleitete.[669] Diese Übermittlungen können nicht mehr dem Grundsatz der Verhältnismäßigkeit genügen und verstoßen daher gegen das Grundgesetz.[670]

Auf Grundlage der Beweisaufnahme durch Aktensichtung und Zeugenbefragung ist belegt, dass in der BND-Abhörstation in Bad Aibling die aus der Fernmeldeaufklärung

667) BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015, 1, A, II), https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/; *Löwnau*, Protokoll-Nr. 114 I, S. 12.

668) BVerfGE 65, 1, (44 ff. und 62), https://openjur.de/u/268440.html; vgl. auch *Schaar*, Protokoll-Nr. 31 I, S. 24.

669) Vermerk der BND-Datenschutzbeauftragten H. F. v. 20. August 2013, MAT A BND-1/6a, Bl. 239 (VS-NfD).

670) BVerfGE 100, 313, Leitsatz Nr. 6, https://www.bverfg.de/e/rs19990714_1bvr222694.html.

gewonnen Metadatenströme direkt und mittels automatisiertem Verfahren in das Verbindungsbüro der NSA, namentlich Special US Liaison Activity Germany (SUSLAG) weitergeleitet werden.[671]

Dieses „ist mit dem Gebäude 8, in dem sich u. a. die IT-Server des BND befinden, per Lichtwellenleiter verbunden. Es besteht eine physikalische 100 Mbit/s-Verbindung zwischen dem Serverraum in Bad Aibling und dem *SUSLAG*-Gebäude. Vom *SUSLAG* besteht auch eine technische Verbindung zum *US-European Technical Center* (*ETC*) in Wiesbaden. Der Datenaustausch zwischen der Dienststelle des BND in Bad Aibling und dem *ETC* Wiesbaden erfolgt via *SUSLAG*."[672] Die NSA-Verbindungsstelle ist weiterhin direkt an das NSA-Netz angebunden.[673] und so liefen die Datenströme „dann von *JAC* über *SUSLAG* nach Amerika."[674]

Die vom BND erfassten Daten wurden vorher – so stellte es der BND für die Operation EIKONAL dar – in verschiedene Stränge von Materialarten aufgeteilt. Nach einigen Zeugenaussagen „gab [es] aus dem gemeinsamen Betriebsgebäude einen Ausgang, der von uns – sprich: BND – gefiltert wurde. Nach dieser Filterung ist dann der Datenstrom aufgesplittet worden und ist einmal dem AND zur Verfügung gestellt worden und erst dann in die Blechdose gegangen und zum Zweiten uns für die interne weitere Verarbeitung."[675] Später bestätigten BND-Zeug_innen, dass diese internen Verarbeitungsschritte, wie Auswertung und Analyse im Betriebsgebäude des JSA gleichwohl gemeinsam mit der NSA vorgenommen wurden. Dort gab es auch ein gemeinsames Netz,[676] zumindest bis Herbst 2007. Laut Zeugenaussagen ist ein Teil der G 10-Filterung erst händisch in Bad Aibling vorgenommen worden.[677] Insbesondere wurden gemeinsame Datenbanken, in denen sich sowohl Daten des BND, als auch der NSA

---

671) *R. U.,* Protokoll-Nr. 14 I, S. 38.

672) Vgl. BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015, 1, A, VI, 1, a), https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/.

673) Antwort des BND vom 2. August 2013 auf eine Anfrage des *Spiegel*, MAT A BND-1/13f, Bl. 240 (VS-NfD).

674) *Breitfelder*, Protokoll-Nr. 28 I, S. 88; das Joint Analysis Center (JAC) soll neben der JSA ein weiterer Übergabepunkt der NSA in Bad Aibling (gewesen) sein.

675) *T. B.*, Protokoll-Nr. 24 II – Auszug offen, S. 33.

676) *T. B.,* Protokoll-Nr. 24 II – Auszug offen, S. 34.

677) *Burbaum,* Protokoll-Nr. 24 II – Auszug offen, S. 9.

befanden, auch gleichermaßen von beiden Parteien genutzt.[678] Somit hatten NSA-Mitarbeiter_innen mindestens für einen bestimmten Zeitraum auch schon vor der Beendigung des Filterprozesses Zugriff zu den Daten (siehe hierzu auch das Kapitel V.6 – „Zu Risiken und Nebenwirkungen…“).

Neben dem automatisierten Datenaustausch stellt die zum Teil integrierte gemeinschaftliche Datenauswertung mit Partner_innen eine in Quantität wie Qualität völlig neue Dimension eines sicherheitsbehördlichen Verfahrens dar. Es lehnt sich ersichtlich an die Konzepte der NSA – mit deren Unterstützung es auch errichtet wurde – an.

Der Metadatenstrang bei der Operation EIKONAL „blieb eben auch liegen auf diesen gemeinsamen Systemen von der *JSA*.“[679] Auf Nachfrage, ob die Daten dort direkt von der NSA abgegriffen wurden, antwortete die Zeugin *K. L.*: „So war das Setup (…) Ob sie tatsächlich abgegriffen wurden, weiß ich nicht, weil, wie gesagt, im Nachgang erzählen die alle: „Das war alles nur Testbetrieb.“[680] Der „Wirkbetrieb“ begann nach Angaben von BND-Zeugen ab Mitte/Ende 2007 und lief bis zur Einstellung der Operation im Juni 2008.[681]

Die Gewährung eines Zugriffsrechts auf den Datenbestand des BND zugunsten der NSA hat sich auch nach BND-internen Ansichten an dem engen Maßstab des § 11 BNDG i. V. m. § 10 BDSG zu orientieren. Die Einrichtung eines automatisierten Abrufverfahrens ist hiernach unzulässig.[682] Auch die Behauptung, der Vorgang finde innerhalb eines – jahrelangen – Testbetriebs statt, ändert an der Rechtslage nichts. Selbst wenn die NSA diesen Zugriff nicht selbst gehabt hätte, so standen ihr immer noch alle Metadaten des BND – ohne eine vergleichbare Vorauswahl – „zur Verfügung“, da ihr komplette Datenströme mit Metadaten aus ganzen Strecken bereitgestellt wurden. In der Praxis ist hier letztlich kein Unterschied erkennbar. Die NSA konnte somit selbst entscheiden, wann sie auf welche BND-Datensätze zugreift, was einer Selbstbedie-

678) *T. B.*, Protokoll-Nr. 20 I, S. 40.

679) *K. L.*, Protokoll-Nr. 30 II – Auszug offen, S. 120.

680) *K. L.*, Protokoll-Nr. 30 II – Auszug offen, S. 121.

681) *S. L.*, Protokoll-Nr. 26 I, S. 66.

682) Antwortentwurf auf BfDI-Anfrage i. V. m. Medienberichten vom 22. Juli 2013, MAT A BND-1/6a, Bl. 92 (VS-NfD).

nung gleichkommt. Es handelt sich hierbei längst nicht mehr um einzelne Übermittlungen. Eine vorherige Selektion der Daten durch den BND fand gerade nicht statt. Der NSA wurden die Daten mittels eines technischen Prozesses automatisiert weitergeleitet, sowie in gemeinsamen Netzen zur Bearbeitung verfügbar gemacht. Dieses Verfahren ist mit dem Grundsatz der Verhältnismäßigkeit nicht vereinbar.[683]

ee) BND handelte ohne Rechtsgrundlage

Der BND greift aufgrund seiner Praxis der Datenerhebung, Speicherung und anschließenden Übermittlung massenhaft in Freiheitsrechte ein. Er verwehrt den verfassungsrechtlich gewährleisteten Schutz des durch Art. 10 GG geschützten Fernmeldegeheimnisses und verletzt das Grundrecht der Betroffenen auf Privatsphäre, auf informationelle Selbstbestimmung sowie die Integrität und Vertraulichkeit informationstechnischer Systeme.

Dieser Eingriff bedarf einer speziellen, eng gefassten, formell-gesetzlichen Ermächtigungsgrundlage, die den Geboten der Bestimmtheit und Verhältnismäßigkeit genügt.[684] Der BND stützt seine Maßnahmen der strategischen Ausland-Ausland-Fernmeldeaufklärung auf die §§ 1 Abs. 2 S. 1 und 2 Abs. 1 BNDG[685], sofern er der Auffassung ist, die Datenerhebung findet im Geltungsbereich des BNDG statt (zur Weltraumtheorie siehe weiter unten V.9.a)gg)aaa)). Übermittlungen an ausländische öffentliche Stellen stützt er in diesen Fällen auf § 9 Abs. 2 BNDG und der sich daraus ergebenden Übermittlungsvorschriften, insbesondere aus dem BVerfSchG. Das BNDG stellt jedoch keine hinreichende Rechtsgrundlage für solche Beschränkungsmaßnahmen des BND dar.[686] (Vgl. Kapitel V.3) Auch die hin und wieder vorgebrachten Vereinbarungen im Memorandum of Agreement (MoA) zwischen dem BND und der NSA[687] können

683) Vgl. *Schaar*, Protokoll-Nr. 31 I, S. 24.

684) Vgl. etwa *Huber*, NJW 2013, 2572 ff.; *Caspar*, PinG 2014, H. 1, S. 4 f.; *Bäcker*, MAT A SV-2/3, S. 16 ff.; *Papier*, MAT A SV-2/2, S. 6 f. und *Hoffmann-Riem*, MAT A SV-2/1, S. 10 ff., 20.

685) Vgl. Bundestagsdrucksache 17/9640, S. 6, 10; 17/14739, S. 9, 14; *Graulich*, MAT A SV-11/2, S. 61 ff.

686) Vgl. *Schaar*, Protokoll-Nr. 31 I, S. 27.

687) *T. B.*, Protokoll-Nr. 24 II, S. 33.

keine Rechtsgrundlage darstellen und den BND nicht von der Einhaltung von Übermittlungsvorschriften entbinden. Dieser bedarf es explizit, wenn der BND Daten übermittelt, die er durch Eingriffe in das Telekommunikationsgeheimnis erlangt hat.[688] Die Übermittlungen von Aufkommen unterfallen auch hier dem Geltungsbereich des Art. 10 GG und hätten daher ausschließlich auf der Grundlage des Artikel 10-Gesetzes erfolgen dürfen. Mangels gesetzlicher Eingriffsgrundlage (vgl. Kapitel V.3.b)bb) – Fernmeldegeheimnis als verfassungsrechtlicher Maßstab) sind die massenhaften Erfassungen und Übermittlungen des BND an die NSA allein schon aus formellen Gründen eindeutig verfassungswidrig zu werten.

Bundesregierung und BND halten weiter an ihrer Interpretation fest, die in Art. 10 GG verankerte Telekommunikationsfreiheit schütze nur deutsche Staatsbürger_innen und Personen mit Aufenthalt in der Bundesrepublik Deutschland. Da der BND zwischen Daten aus der Ausland-Ausland-Aufklärung und G 10-Daten unterscheidet und es sich seiner Ansicht nach bei der Metadatenerfassung im Rahmen von EIKONAL und der Satellitenerfassung in Bad Aibling lediglich um Auslandsverkehre handelt, setzt er hieran, sowie an alle darauffolgenden Verarbeitungsschritte einschließlich der Übermittlung einen weitaus geringeren rechtlichen Maßstab. Aufgrund der automatischen Weiterleitung kompletter Metadatenströme und eines mangelhaften vorgeschalteten Filtersystems konnte der BND die Einhaltung selbst dieses eingeschränkten Schutzbereichs von Artikel 10 GG nicht garantieren. Die Behauptungen des BND, es handele sich lediglich um ausländische TK-Verbindungen und personenbezogene Daten deutscher Staatsbürger seien nicht betroffen, sind durch Erkenntnisse des Untersuchungsausschusses wiederlegt worden. Der BND konnte folglich überhaupt nicht gewährleisten, dass deutsche Staatsbürger und Kommunikationsverbindungen mit Inlandsbezug nicht von der Datenweitergabe betroffen waren. Er kann sich daher auch nicht nach BND-eigener Rechtsauffassung aus seiner Verantwortung und der Verpflichtung zur Einhaltung des Grundgesetztes entziehen.

688) *Papier*, Beschränkungen der Telekommunikationsfreiheit durch den BND an Datenaustauschpunkten, NVwZ-Extra 15/2016, S. 1 (14), abrufbar unter http://rsw.beck.de/rsw/upload/NVwZ/NVwZ-Extra_2016_15.pdf.

Der grundrechtliche Schutzumfang der Telekommunikationsfreiheit besitzt vielmehr eine große Reichweite und umfasst insbesondere auch die Metadaten. Denn der Gewährleistungsgehalt von Art. 10 Abs. 1 GG bezieht sich nicht nur auf den Inhalt der geführten Gespräche, sondern auch auf die „näheren Umstände“ der Telekommunikation.[689]

Der BND kann sich auch nicht darauf berufen, dass er sich in den zahlreichen Jahren der Zusammenarbeit bei der Erfassung und Bearbeitung von leitungsgebundenen Verkehren und IP-Verkehren in der betrieblichen Testphase befunden haben soll.[690]

ff) Verstöße gegen Übermittlungsvorschriften aus § 9 Abs. 2 BNDG[691] i. V. m. §§ 19 ff. BVerfSchG[692]

Der BND umging mit seiner Praxis der Datenweiterleitung sämtliche gesetzliche Übermittlungsvorschriften und verstieß gegen seine eigenen Dienstvorschriften.

„[redacted]“[693],

---

689) BVerfGE 67, 157, Beschl. v. 20.06.1984 – 1 BvR 1494/78, abrufbar unter http://www.servat.unibe.ch/dfr/bv067157.html, dort Rn. 54; *Caspar*, Strategische Auslandsüberwachung – Jenseits der Grenze des Rechtsstaats, PinG 2014, H. 1, S. 3 f.

690) Vgl. Interne Weisung betr. JSA, Weitgabe von TK-Verkehren an AND v. 18. Februar 2005, MAT BND-40a, Bl. 7 (VS-NfD).

691) Dies gilt für sämtliche Fassungen des BNDG im Untersuchungszeitraum (30.12.1990 – 31.12.2001, 01.01.2002 – 10.01.2007, 11.01.2007 – 20.11.2015 sowie 21.11.2015 – 30.12.2016).

692) Dies gilt für sämtliche Fassungen des VerfSchG im Untersuchungszeitraum (01.01.2000 – 31.12.2001, 01.01.2002 – 10.01.2007, 11.01.2007 – 09.01.2012 sowie 10.01.2012 – 20.11.2015).

693) BND-interne Bitte um Mitzeichnung einer Leitungsvorlage – Datenaustausch mit US-Stellen, MAT A BND-40a, Bl. 58-62 (58) (VS-NfD).

sie muss sich nur in den Grenzen der §§ 9 Abs. 2 BNDG i. V. m. 19 Abs. 3 BVerfSchG halten.

Der BND umging so bewusst die deutlich engeren Vorschriften des Artikel 10-Gesetzes. Er hielt sich jedoch bei der Metadatenweitergabe nicht einmal an die von ihm selbst für die Metadatenausleitung zu Grunde gelegten Übermittlungsvorschriften i. S. d. § 9 Abs. 2 BNDG i. V. m. § 19 Abs. 3 BVerfSchG.[694] So verstieß der BND vielfach und in gravierendem Maße gegen die sich selbst daraus ergebenden geringeren gesetzlichen Anforderungen. Vor diesem Hintergrund verwundert die Falschaussage des stellvertretenden Regierungssprechers *Georg Streiter*: „Es gibt keine millionenfache Grundrechtsverletzung durch deutsche Geheimdienste“ (…) „Die deutschen Dienste halten sich an die Vorschriften des Datenschutzes“, betonte er. Die Übermittlung personenbezogener Daten an ausländische Stellen erfolge nur in Einzelfällen. 2012 seien dies nur zwei Datensätze gewesen, die ein und dieselbe Personen betroffen hätten.[695] Bei den hier in Rede stehenden Datensätzen handelt es sich um Übermittlungen, die der BND nach dem Artikel 10-Gesetz behandelte. Damit sollte wohl die dahinterliegenden massenhaften Metadatensätze verschleiert werden, bei deren Übermittlung sich der BND nicht an die Vorschriften hielt. Untersuchungen des Ausschusses haben jedoch ergeben, der BND hielt sich nicht nur nicht an Vorschriften, sie sind ihm zum Teil noch nicht einmal bekannt gewesen.[696] (vgl. auch Kapitel V.1 zum MoA) Allgemein bekundete die Datenschutzbeauftragte des BND *Dr. H. F.* vor dem Ausschuss, dass „einfach eine große Unkenntnis zum Thema „Datenschutz und Datenschutzrecht“ in der Abteilung [Technische Aufklärung] vorhanden war.“[697] Die BfDI stellte sogar in Folge eines Kontrollbesuchs der Außenstelle in Bad Aibling hinsichtlich allgemeiner Kernbereiche der Aufgabenerfüllung des BND 18 Rechtsverstöße und 12 förmliche Beanstandungen gemäß § 25 Abs. 1 S. 1 BDSG fest.[698]

---

694) MAT A BND-1/6a, Bl. 79 (VS-NfD).

695) *Reuters* vom 5. August 2013, „Bundesregierung gibt BND in Späh-Affäre Rückendeckung“, http://de.reuters.com/article/schland-usa-spionage-idDEBEE97403I20130805, abgerufen am 17. Juni 2017.

696) *H. F.*, Protokoll-Nr. 121 I, S. 8.

697) *H. F.*, Protokoll-Nr. 121 I, S. 7.

698) BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015, https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/, abgerufen am 17. Juni 2017.

aaa) Metadaten sind regelmäßig personenbezogene Daten

Metadaten sind zweifelsohne regelmäßig personenbezogen bzw. personenbeziehbar und damit personenbezogene Daten im Sinne der gemäß § 11 BNDG geltenden Legaldefinition des § 3 Abs. 1 BDSG. Demnach handelt es sich bei personenbezogene Daten um „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)“. Der von Nachrichtendiensten benannte Zweck bestimmter Datenerfassungen, ist für die Bestimmung des Personenbezugs ebenso wenig relevant,[699] wie der Ursprung des Datums. Auch kann die konkrete Beschaffenheit sowie die Art und Weise der Darstellung von Informationen keinen Einfluss hierauf haben.[700]

Hierfür muss lediglich ein Bezug zu den persönlichen oder sachlichen Verhältnissen einer Person hergestellt werden können. Für die Eingriffsqualität ist also zunächst nicht entscheidend, ob die erfassten Daten sofort bestimmten Personen zuzuordnen sind.[701] „Schon die Möglichkeit der Herstellung dieses Personenbezugs, die generell jedenfalls vorhanden ist – das gilt auch für Auslandsverkehre –, führt dazu, dass man den Datenbestand, der dort verarbeitet wird, als personenbezogen anzusehen hat.“[702] Bei der Erfassung und Übermittlung von Metadaten, konnte der BND gerade nicht ausschließen, auch solche personenbezogenen Daten zu behandeln. Dies wurde vor dem Untersuchungsausschuss vom früheren BfDI, *Peter Schaar*, bekräftigt:

> „Metadaten sind im Regelfall personenbezogene Daten, weil sie so wie das Internet und auch die Mobilfunknetze funktionieren, letztlich immer sich auf Sender und Empfänger beziehen. Und dabei handelt es sich häufig um natürliche Personen.“[703]

---

699) BVerwG, Urteil vom 24. Mai 2010 – 6 A 2.09 –, Rn. 33, www.bundesverwaltungsgericht.de/entscheidungen/entscheidung.php?lang=de&ent=240310U6A2.09.0, abgerufen am 11. Juni 2017.

700) *Dammann*, in: Simitis, Bundesdatenschutzgesetz, 6. Auflage, 2006, § 3, Rn. 4; BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015, 1, A, I, 1, a, aa), https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/, agerufen am 17.06.2017.

701) BVerfGE 100, 313 (366), https://www.bverfg.de/e/rs19990714_1bvr222694.html.

702) *Schaar*, Protokoll-Nr. 31 I, S. 10.

703) *Schaar*, Protokoll-Nr. 31 I, S. 24.

Auch die Zeugin *Gabriele Löwnau,* Referatsleiterin bei der BfDI, erklärte:

> „Also, da bin ich der Überzeugung – ich habe ja auch mal im Telekommunikationsbereich gearbeitet-, dass natürlich ein Teil der Metadaten personenbeziehbar ist, und das reicht nach BDSG. Natürlich gibt es da auch, bei diesen Metadatensätzen, irgendwelche signalisierungstechnischen Daten, die nicht personenbeziehbar sind; aber das ist ja nur ein Teil.“[704]

Die Zeugin *Polzin*, Leiterin des Referats 601 im Kanzleramt, welches zuständig ist für das Recht der Nachrichtendienste, verdeutlichte dies:

> „Sie können personenbezogen sein. Sie können personenbeziehbar sein. Es kommt darauf an. Man kann jedenfalls nicht ausschließen, dass sie personenbezogen sind.“[705]

Aufgrund dessen hätte der BND sämtliche Metadaten als personenbezogene Daten behandeln müssen.

Das Gesetz kennt bezüglich der Übermittlung personenbezogener Daten auch kein erlaubtes Risiko. Insoweit sind auch weitere Übermittlungen durch die NSA an Dritte sowie deren Möglichkeit zur Personenzuordnung einzubeziehen. Dennoch nahm der BND das Risiko einer Personenbestimmung durch die NSA in Kauf. Realisiert sich dieses später, so hat er, da keine Übermittlungsbefugnis bestand, rechtswidrig personenbezogene Daten übermittelt. „Der Umstand, dass ein Personenbezug ex ante betrachtet mit verhältnismäßigen Mitteln nicht herzustellen erschien, befreit nicht von der datenschutzrechtlichen Haftung, wenn dieser Fall dennoch eintritt […]. Die Stelle kann sich nicht darauf berufen, sie habe das Risiko auch bei sorgfältiger Prüfung nicht erkennen können.“[706] Der BND hätte daher vorsorglich alle übermittelten Daten wie personenbezogene Daten behandeln müssen. Insbesondere vor dem Hintergrund, dass er wusste, dass die NSA besondere Methoden zur Metadatenanalyse besitzt.

---

704) *Löwnau*, Protokoll-Nr. 72 I, S. 44.

705) *Polzin*, Protokoll-Nr. 72 I, S. 144.

706) *Dammann*, in: *Simitis*: Bundesdatenschutzgesetz, § 3, Rn. 38.

Nach der Rechtsprechung des *Bundesverfassungsgerichts* „gibt es unter den Bedingungen der elektronischen Datenverarbeitung kein schlechthin, also ungeachtet des Verwendungskontextes, belangloses personenbezogenes Datum (…) Auch entfällt der grundrechtliche Schutz nicht schon deshalb, weil die betroffene Information öffentlich zugänglich ist“.[707] Die Legaldefinition in § 3 Abs. 1 BDSG umfasst auch personenbezogene Angaben „mit geringer Aussagekraft“.[708]

bbb) Fehlende Erforderlichkeitsprüfung

Gemäß § 9 Abs. 2 BNDG i. V. m. § 19 Abs. 3 S. 1 BVerfSchG darf der BND personenbezogene Daten an ausländische öffentliche Stellen übermitteln, soweit „die Übermittlung zur Erfüllung seiner Aufgaben oder zur Wahrung erheblicher Sicherheitsinteressen des Empfängers erforderlich ist“.[709] Der BND verstieß vielfach und in gravierendem Maße gegen dieses Element der Erforderlichkeitsprüfung.

Der BND hat im Zusammenhang mit den Übermittlungen der Metadaten eine Erforderlichkeit nicht nur nicht feststellen können, er hat sie noch nicht einmal geprüft. Im Gegenteil, er leitete alle Daten automatisiert an die NSA weiter, ohne zu wissen, welche Daten im Datenstrom enthalten waren. Eine Prüfung der Erforderlichkeit kann auch nicht pauschal erfolgen, sondern muss für jede einzelne Übermittlung vorgenommen werden.[710] Das der Zusammenarbeit zugrundeliegende Tauschgeschäft des BND mit der NSA kann diesen fehlenden Erforderlichkeitstatbestand nicht decken, es ist vielmehr als Ursache der rechtswidrigen Handlungen zu werten. Aufgrund von Art und Umfang der übermittelten Daten, ist davon auszugehen, dass in zahlreichen Fällen, eine Übermittlung an einer fehlenden Erforderlichkeit gescheitert wäre. Der BND gab

707) BVerfGE 120, 378-433, Rn. 66 f., https://www.bverfg.de/e/rs20080311_1bvr207405.html; BVerfGE 65, 1-71, Rn. 176 (Volkszählungsurteil), https://openjur.de/u/268440.html.

708) *Dammann*, in: *Simitis*, Bundesdatenschutzgesetz, § 3, Rn. 8; BVerfGE 120, 378-433, https://www.bverfg.de/e/rs20080311_1bvr207405.html; vgl. BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015, 1, A, I, 1, a, aa), https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/

709) Vgl. DV Übermittlung, Nr. 3.2.1., MAT A BND-6b, Bl. 94f. (VS-NfD).

710) Vgl. BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015, 1, G), https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/.

somit massenhaft Daten über Kommunikationsverkehre unbescholtener Personen an die NSA weiter.

Auch BND-intern wurden rechtliche Zweifel hinsichtlich der Übermittlungspraxis an die NSA erhoben. So hielt die Datenschutzbeauftragte des BND *Dr. H. F.* in einem internen Schreiben vom 20. August 2013 fest:

> „[redacted][711]

ccc) Keine Prüfung vor Übermittlung auf entgegenstehende Interessen

Nach Untersuchungen des Ausschusses hat der BND aller Wahrscheinlichkeit nach auch Daten an die NSA übermittelt, die gegen deutsche und/oder europäische Interessen verstießen. Aufgrund der bei der Satellitenüberwachung in Bad Aibling ausgewählten Strecken kommen wir zu der begründeten Annahme, dass auch solche Metadaten im übermittelten Datenstrom enthalten waren.

Eine solche Übermittlung hätte gemäß § 19 Abs. 3 S. 2 BVerfSchG nie stattfinden dürfen. Demnach muss eine Übermittlung nämlich unterbleiben, sobald Anhaltspunkte bestehen, dass „auswärtige Belange der Bundesrepublik Deutschland oder überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen“. Die massenhaft ausgeleiteten Metadaten wurden, bis auf ein Durchlaufen einer automatisierten Filterung, keiner Prüfung unterzogen. Ein Filterkriterium, das deutsche und europäische Interessen in dem Sinne berücksichtigt hätte, dass keine (Meta-)Daten von Regierungen und Einrichtungen der EU, ihrer Mitgliedstaaten oder europäischer Firmen aussortiert hätte, gab es vor März 2015 nicht (siehe hierzu Kapitel V.8 – Verstöße bei der Verwendung von Suchbegriffen/Selektoren der NSA).

711) Vermerk der BND-Datenschutzbeauftragten H. F. v. 20. August 2013, MAT A BND-1/6a, Bl. 239-241 (240) (VS-NfD).

Dem genannten internen Vermerk der BND-Datenschutzbeauftragten Dr. *H. F.* vom 20. August 2013 ist zu entnehmen:

> „Eine inhaltliche Sichtung bzw. eine Eingrenzung der erhobenen Daten anhand von wie auch immer gearteten Kriterien finde nicht statt. Stattdessen würden alle auf den betreffenden Strecken erhobenen Daten – bereinigt um Daten mit Deutschlandbezug – an *USA-SUSLAG* weitergegeben.“[712]

Auf die Argumentation des Rechtsreferats der Abteilung Technische Aufklärung (TAG), dass durch die Ausgestaltung der technischen Systeme die Voraussetzungen der §§ 9 BNDG und 19 BVerfSchG erfüllt würden, merkte sie weiter an:

> „[redacted]“[713]

Nach der BND-internen Dienstvorschrift obliegt „[redacted]“[714] Vorliegend bleibt bereits fraglich, wer diese Aufgabe bei einer automatisierten Weiterleitung übernimmt. Gesetzlich gefordert ist eine Einzelfallüberprüfung und -abwägung, bei der die jeweiligen konkreten Einzelfallumstände Berücksichtigung finden.[715]

---

712) Vermerk der BND-Datenschutzbeauftragten H. F. v. 20. August 2013, MAT A BND-1/6a, Bl. 239-241 (239) (VS-NfD).

713) Handschriftliche Notiz von *H. F.* auf dem Schreiben TAG vom 28. August 2013, MAT A BND-1/6a, Bl. 274 f. (275) (VS-NfD).

714) DV Übermittlung, Nr. 3.2.2, MAT A BND-6b, Bl. 95 (VS-NfD).

715) *Droste*, Handbuch der Verfassungsschutzrechts, Stuttgart u.a. 2007, S. 534; vgl. die Aussage von *H. F.*, Protokoll-Nr. 16 I, S. 67.

„[redacted]"[716] so die Dienstvorschrift „Übermittlung" des BND. Nach dem vorliegenden automatisierten Weitergabeverfahren war es jedoch überhaupt nicht möglich, dass ein solcher Anlass zur Vermutung überhaupt nur entstehen konnte. Dies schien für den BND auch nicht nötig. Er bemühte sich lieber um eine pauschale Abwägung aller Interessen und argumentierte schon im Jahr 2002: „[redacted]"[717] Diese pauschale Abwägung ist mit deutschem Recht nicht vereinbar, da sie gegen § 19 BVerfSchG als einfachgesetzliche Ausprägung des Gebots der Verhältnismäßigkeit verstößt.[718] Sie ist insbesondere auch vor dem Hintergrund unhaltbar, dass der BND bereits im Jahr 2002 feststellte, dass seine automatisierten Aus- und Weiterleitungen von Rohmaterial ganzer Strecken Daten enthalten, die gegen deutsche bzw. europäische Interessen verstoßen. Auf Unkenntnis kann sich der BND nicht berufen.

Angesichts der technischen Entwicklung zu IP-Verkehren kann von einer vermuteten „vereinzelten Weitergabe" keine Rede sein.

ddd) Keine Prüfung entgegenstehender Übermittlungsverbote

Der BND nahm entgegen seiner Verpflichtung keine Prüfung entgegenstehender Übermittlungsverbote vor.

Er hätte gemäß § 10 BNDG i.V.m. § 23 Nr. 1 BVerfSchG die Daten vor der Übermittlung unter Berücksichtigung der Art der Informationen und ihrer Erhebung auf ein –

716) DV Übermittlung, Nr. 3.2.2, MAT A BND-6b, Bl. 95 (VS-NfD).

717) Interne Vorlage für den AL2 vom 31. Juli 2002, betr. „Rohmaterialaustausch mit AND'en", hier: G 10-Problematik / Wahrung deutscher bzw. europäischer Interessen, MAT BND-40a, Bl. 15-19 (15) (VS-NfD).

718) *Bock*, in: *Schenke/Graulich/Ruthig*, Sicherheitsrecht des Bundes, 2014, BVerfSchG, § 19, Rn. 21.

dem Allgemeininteresse überwiegendes – schutzwürdiges Interesse der/s Betroffenen prüfen müssen. Dies unterließ der BND.

Im Hinblick auf die Interessen von Betroffenen ist eine fehlende Überprüfung insbesondere im Zusammenhang mit der auch dem BND bekannten Verwendung von Metadaten durch die NSA (vgl. Kapitel XII – Beteiligung Deutschlands am US-Drohnenkrieg) ein besonders schwerwiegender Rechtsverstoß. Mögliche Folgemaßnahmen beim Datenempfänger gegen die Betroffenen bis hin zu extralegalen Tötungen mussten vom BND mitberücksichtigt werden.

Auch der Schutz von Minderjährigen wurde vom BND missachtet. Die Übermittlung von Informationen einschließlich personenbezogener Daten über das Verhalten Minderjähriger – vor der Vollendung des 16. Lebensjahres – an einen anderen Nachrichtendienst war gemäß § 10 BNDG in Verbindung mit § 24 Abs. 2 BVerfSchG unzulässig. Der BND hat die Daten von Minderjährigen nicht unter Beachtung der „Umstände des Einzelfalls“ gemäß § 24 Abs. 2 S. 2 BVerfSchG geprüft und anschließend aussortiert, sondern einheitlich mit dem Datenstrom an die NSA übermittelt.

Gemäß § 10 BNDG in Verbindung mit § 24 Abs. 1 BVerfSchG könnte dies in einzelnen Fällen zulässig sein.[719] Der BND erfüllte jedoch weder die in §24 BVerfSchG bezeichneten Voraussetzungen einer Speicherung nach § 11 BVerfSchG, noch prüfte er die Erforderlichkeit der Speicherung zur Abwehr einer erheblichen Gefahr oder zur Verfolgung einer Straftat von erheblicher Bedeutung. Es besteht somit keinerlei Rechtfertigungsgrund für diese Handlung. Der BND hielt die Verfahrensregeln des § 10 BNDG nicht ein.

Weiterhin fand keine Überprüfung der Daten hinsichtlich einer möglichen Relevanz für einen verbotenen Ringtausch statt. Der BND hat nicht geltend gemacht, dass die Metadaten von US-Bürger_innen und -Institutionen vor der Weitergabe an die NSA aussortiert würden, sondern stets betont, dass die Daten „G 10-gefiltert“ würden. Nach Auflösung der JSA in Bad Aibling im Jahr 2012 seien die in der Kooperation eingesetzten BND-Selektoren nach Angaben von BND-Zeugen auch nicht mehr nach USSID-18, d. h. auf geschützte US-Personen geprüft worden. Wir haben keinerlei Hinweise

719) Vgl. DV Übermittlung, Nr. 5.2, MAT A BND-6b, Bl. 105 (VS-NfD).

darauf, dass dies bei den Datenübermittlungen an die NSA anders als bei den Selektoren gehandhabt wurde.

Nach internen Übermittlungsvorschriften dürfte der BND die Daten auch nicht weiterleiten, „[redacted]".[720] Mit Blick auf die fehlenden Dateianordnungen hätten diese gelöscht werden müssen (s. o. V.9.a)cc) – Rechtswidrigkeit aufgrund fehlender Dateianordnungen) Es bestand danach auch ein Übermittlungsverbot nach den internen Datenübermittlungsvorschriften.

eee) Keine Zweckbindung für Weiterverwendung durch NSA

Gemäß § 9 Abs. 2 BNDG i. V. m. § 19 Abs. 3 S. 4 BVerfSchG ist der Empfänger „darauf hinzuweisen, dass er die übermittelten Daten nur zu dem Zweck verwenden darf, zu dem sie ihm übermittelt wurden und dass der Bundesnachrichtendienst sich vorbehält, um Auskunft über die vorgenommene Verwendung der Daten zu bitten."[721] Die Übermittlung von Daten an staatliche Stellen im Ausland unterliegt den allgemeinen verfassungsrechtlichen Grundsätzen von Zweckänderung und Zweckbindung.[722]

Der BND übermittelte die Metadaten ohne eine solche Zweckbindung an die NSA. Auf die Frage, ob in der Praxis in Bad Aibling bei den Datenübermittlungen ein sog. Disclaimer verwendet werde, um die Zweckbindung zu erreichen, verneinte dies der Zeuge *J. Z.*:

> „Es wird ja der Datenstrom übermittelt. Wir haben ja jetzt kein Dokument, wo wir das noch drunter drucken können, sonst müssten wir die Sachen ja vielleicht ausdrucken. Also, nein, das ist nicht erfolgt."[723]

Ein Disclaimer werde nur im Schriftverkehr genutzt.

---

720) Vgl. DV Übermittlung, Nr. 3.2.2, MAT A BND-6b, Bl. 95 (VS-NfD)

721) Vgl. DV Übermittlung, Nr. 3.2.3, MAT A BND-6b, Bl. 96 (VS-NfD); MAT A BND-40a, Bl. 11 (VS-NfD).

722) BVerfGE 141, 220-378, Ls. 3, https://www.bverfg.de/e/rs20160420_1bvr096609.html.

723) *J. Z.*; Protokoll-Nr. 14 II – Auszug offen, S. 75.

Weiterhin gaben einige Zeugen bei der Befragung an, dass es keine konkreten Anhaltspunkte für eine Missachtung der Zweckbindung gäbe. Grund hierfür ist vor allem, dass der BND bis zum Spätsommer 2013 in den seltensten Fällen um Auskunft über die vorgenommene Verwendung bat und somit auch nie überprüfte, auf welche Art und Weise die NSA die Daten für welche Zwecke verwendete. Eine Vergewisserung wäre jedoch auch nach der Rechtsprechung des BVerfG geboten gewesen. So ist bei der Beurteilung der neuen Verwendung, auf die Eigenständigkeit der anderen Rechtsordnung zu achten. „Eine Übermittlung von Daten ins Ausland verlangt eine Vergewisserung darüber, dass ein hinreichend rechtsstaatlicher Umgang mit den Daten im Empfängerstaat zu erwarten ist.“[724] Dies ist besonders kritisch zu werten vor dem Hintergrund, da es nicht vollumfänglich nachvollziehbar ist, für welche Daten sich die NSA tatsächlich interessierte und wie sie diese verwendete. Die NSA hatte kein Interesse daran, den BND darüber vollends aufzuklären. Dabei lagen dem BND – wie auch jedem Zeitungsleser auch – Hinweise auf eine missbräuchliche Verwendung der Daten seitens der NSA und anderer US-Dienste vor (siehe Kapitel XII – Beteiligung Deutschlands am US-Drohnenkrieg).

Datenübermittlungen sind gleichsam nur zulässig, solange sie an Staaten weitergegeben werden, in denen ein Datenschutzniveau gewährleistet ist, das mindestens dem der Bundesrepublik Deutschland entspricht und die Verwendung der Daten durch die NSA „in einer adäquaten rechtsstaatlichen Art und Weise erfolgt“.[725] In Bezug auf die USA habe die BfDI offenbar schon 2007 Bedenken bei der Annahme eines solchen vergleichbaren Datenschutzniveaus geäußert.[726] Auch im BND hieß es intern, es lasse sich „[redacted].“[727]

724) BVerfGE 141, 220-378, Ls. 3, https://www.bverfg.de/e/rs20160420_1bvr096609.html.

725) *Papier*, Beschränkungen der Telekommunikationsfreiheit durch den BND an Datenaustauschpunkten, NVwZ-Extra 15/2016, S. 1 (14), abrufbar unter http://rsw.beck.de/rsw/upload/NVwZ/NVwZ-Extra_2016_15.pdf.

726) MAT A BND-40a, Bl. 24 (VS-NfD).

727) E-Mail vom 29. August 2008, MAT A BND-40a, Bl. 49 (VS-NfD).

fff) Keine Dokumentation

Die Übermittlung ist gemäß § 9 Abs. 2 BNDG i. V. m. § 19 Abs. 3 S. 3 BVerfSchG aktenkundig zu machen, d. h. „über die Vorgänge sind schriftliche Unterlagen zu fertigen und zu sammeln."[728] Der BND protokollierte die Metadatenweitergabe an die NSA nicht, weshalb er nach eigenen Angaben technisch nicht mehr nachvollziehen konnte, wann wie viele Daten welchen Inhalts abgeflossen sind. Nach Zeugenaussagen war eine Protokollierung auch gar nicht möglich, denn „wenn Sie alle Daten dokumentieren müssten, die Sie dann austauschten, dann haben Sie eine riesige Datenhaltung."[729] Auch die Referatsleiterin 601 im Kanzleramt, Frau *Polzin*, gestand zu, „dass der § 19 Absatz 3 [BVerfSchG] nicht an Millionen oder Milliarden sicherlich gedacht hat. Aber man hätte sich dem durchaus sehr gut anpassen können."[730] Die Frage nach dem Wie bleibt. Die Durchführung von vollständigen Einzelfallprüfungen erscheint bei dieser Menge schlicht nicht möglich. So blieb es dabei: „Wir wissen, auf welchen Strecken wir uns bewegen, und wir wissen, seit wann wir da drauf sind. Und das ist es im Großen und Ganzen." Auf weitere Nachfragen äußerte der Zeuge *H. K.* jedoch, dass er es schlicht gar nicht wisse, ob eine Dokumentation in irgendeiner Weise stattfinde.[731] Es handelte sich somit um bloße Vermutungen der Mitarbeiter_innen.

Auch die dem Ausschuss erst aufgrund eines weiteren von der Opposition erwirkten Beweisbeschlusses (BND-54) „ohne Anerkennung einer Rechtspflicht" vorgelegten Statistiken zur Meta- und Inhaltsdatenübermittlung an die NSA für den Zeitraum Oktober 2013 bis März 2014 und tabellarischen Aufstellungen der ausgeleiteten Satelliten-Strecken[732] ab 2013 erfüllen nicht die Anforderungen des „Aktenkundigmachens", sie sind keine Dokumentation im Sinne des § 9 Abs. 2 BNDG i. V. m. § 19 Abs. 3 S. 3 BVerfSchG. Anhand einer bloßen Tabelle, in der tageweise die Gesamtanzahl der übermittelten Metadaten in Millionenhöhe aufgeführt ist, lässt sich gerade nicht nachvollziehen, ob und mit welchen Abwägungen Daten an die NSA übermittelt wurden.

728) Vgl. DV Übermittlung, Nr. 3.2.5, MAT A BND-6b, Bl. 96 (VS-NfD).

729) *H. K.*, Protokoll-Nr. 81 I, S. 8.

730) *Polzin*, Protokoll-Nr. 72 I, S. 156.

731) *H. K.*, Protokoll-Nr. 81 I, S. 23.

732) Siehe MAT A BND-54 (Tgb.-Nr. 235/16 – GEHEIM).

Für die vorgelegten Übersichten zur Streckenbelegung gilt dies gleichermaßen; zudem scheinen sie auch nur einen Bruchteil der Strecken zu umfassen, die die BfDI bei ihrem Kontrollbesuch in Bad Aibling festgestellt hat. Statistiken über Metadatenübermittlungen an die NSA wurden vor Herbst 2013 nach Angaben des BND gar nicht geführt.[733] D .h. für die Vorjahre gab es nicht einmal eine zahlenmäßige Erfassung des Übermittlungsumfangs.

Der BND verhinderte folglich schon im Ansatz eine Rekonstruktion und somit auch Überprüfbarkeit seiner Handlungen.

Zudem hätte der BND „unvollständig oder unrichtig“ übermittelte personenbezogene Daten „unverzüglich gegenüber dem/der Empfänger/in (…) berichtigen“[734] müssen. Da der BND bereits die Übermittlung nicht aktenkundig machte, konnte er jedoch auch eine solche Nachberichtspflicht nicht leisten.

Die fehlende Protokollierung stellt einen weiteren Rechtsverstoß dar. Aufgrund der Heimlichkeit der Maßnahmen ist ihre Protokollierung durch den BND jedoch umso bedeutsamer.

Als die BfDI im Oktober 2014 bei ihrem Kontrollbesuch in Bad Aibling die in der Datenbank VERAS enthaltenen G 10-gekennzeichneten Metadatensätze einsehen wollte, war ihr dies aufgrund der Datenmenge schier unmöglich. Selbst als sie die Anzeige von 90 Tagen auf den geringstmöglichen Zeitraum von lediglich einem Tag reduzierte, war die Trefferzahl mit über 15.002 Treffern zu groß, um noch angezeigt werden zu können.[735] Wenn nicht einmal solche G 10-Metadaten wegen der großen Menge überprüfbar waren, wie sollte dies bei denen aus Ausland-Auslandsverkehren, die nach Angaben von BND-Zeugen ein Vielfaches der G 10-Daten ausmachten, möglich sein.

---

733) *R. U.*, Protokoll-Nr. 14 I, S. 31; E-Mail von *A. F.* an *H. F* vom 21. August 2013, MAT A BND-40a, Bl. 139 (VS-NfD)

734) Vgl. DV Übermittlung, Nr. 5.3, MAT A BND-6b, Bl. 106 (VS-NfD).

735) BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015, 1, A, IV), https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/.

ggg) Keine Kenntnis des BND über Umfang der erhobenen und übermittelten Daten bis 2013

Der BND betreibt eine exzessive Form der Vorratsdatenspeicherung und besaß dennoch bis zum Spätsommer 2013 keine Kenntnis über den konkreten Umfang erhobener und übermittelter Daten an die NSA. Dies wurde den BND-Mitarbeiter_innen bewusst, als *Der Spiegel* und *Spiegel Online* am 29. und 30. Juni 2013 im Zusammenhang mit den Snowden-Veröffentlichungen zum Programm *BOUNDLESS INFORMANT* konkrete Zahlen der Überwachung durch die NSA veröffentlichten.[736] Danach soll die NSA über 500 Milionen Metadaten pro Monat aus Deutschland erhalten haben. So sagte die Zeugin *Dr. H. F.* aus:

> „Als Herr *Snowden* das Thema ‚Kooperation‘ überhaupt aufs Tapet gebracht hat, haben wir angefangen, uns mit der Zusammenarbeit zwischen der Dienststelle in Bad Aibling und der NSA auseinanderzusetzen, weil ja relativ schnell, wenige Tage danach, die ersten Anfragen der BfDI bei uns auf dem Tisch gelandet sind.“[737]

Das öffentliche Bekanntwerden des enormen Ausmaßes versetzte den BND in große Aufregung. Offiziell erfolgten im Jahr 2012 lediglich drei Übermittlungen von Daten aus der strategischen Fernmeldeaufklärung nach dem Artikel 10-Gesetz, die insgesamt 11 G 10-Meldungen betrafen.[738] Bis zu jenem Zeitpunkt gab es im BND, wie bereits gezeigt, nicht einmal Kenntnis, geschweige denn eine Dokumentation über Art und Umfang der massenhaft weitergeleiteten Daten aus der Ausland-Ausland-Aufklärung.

Einen Tag nach der zweiten Veröffentlichung zu BOUNDLESS INFORMANT, am 30. Juli 2013, forderten bereits das Kanzleramt und der BfDI den BND auf, zu den Vorwürfen Stellung zu beziehen.[739] Da sich dies äußerst schwierig gestaltete, fing der

---

736) *Spiegel Online* vom 30. Juli 2013, „NSA überwacht 500 Millionen Verbindungen in Deutschland“, http://www.spiegel.de/netzwelt/netzpolitik/nsa-ueberwacht-500-millionen-verbindungen-in-deutschland-a-908517.html.

737) *H. F.*, Protokoll-Nr. 121, S. 18.

738) Bericht des PKGr über Beschränkungsmaßnahmen nach den §§ 3, 5, 7a und 8 G 10-Gesetz für 2012, Bundestagsdrucksache 18/218 vom 19. Dezember 2013, S. 9: Übermittlungen nach § 7a G 10.

739) Bspw. E-Mail des Kanzleramtes, Referat 603 an den BND vom 30. Juli 2013, MAT A BND-1/9c, Bl. 227 (VS-NfD).

BND erstmals an, sich mit dieser Berichterstattung auseinanderzusetzen, interne Untersuchungen durchzuführen und Nachfragen zu stellen.

„Wir konnten die Zahl ja erst nicht nachvollziehen“, berichtete der BND-Unterabteilungsleiter *W. K.* vor dem Untersuchungsausschuss.

> „Wir sind ja konfrontiert worden mit dem Artikel: Was ist denn das? Ist das bei euch? – Da wir die Metadaten ja so nicht zählen, haben wir gesagt: Wir können es nicht nachvollziehen, wir müssen aber mal was etablieren, eine Zählmethode, eine Statistik, um das zu zählen. – Genau das ist das. Wir haben dann eben in Bad Aibling von der Software-Unterstützungsgruppe dort mal diese Zählung veranlasst. Das hat ein bisschen gedauert.“[740]

Doch zu mehr Transparenz und besserer Kontrolle führte dies in der Folge nicht.

Der ehemalige BND-Präsident *Schindler* fragte umgehend, am 30. Juli 2013, NSA-Direktor *Keith B. Alexander* in einem Schreiben persönlich, [redacted].“ Aus Sicht des BND erklärten sich die Zahlen insbesondere aus der Zusammenarbeit mit der NSA u. a. zur Force Protection. Unklar seien auch die Höhe der Zahlen und deren Zusammensetzung.[741] Darüber hinaus wollte er gerne den ‚[redacted] sowie das ‚[redacted] erfahren. Weiterhin wollte er wissen, ob die [redacted] und unter ‚[redacted]“ stattfand, ‚[redacted]“ hätte, es ‚[redacted]“ gäbe und ob es sich hierbei um eine ‚[redacted]“ handele. *Schindler* fragte zudem, nach der ‚[redacted]“ und

---

740) *W. K.*, Protokoll-Nr. 22 III – Auszug offen, S. 45

741) Schreiben von Präsident *Schindler* an NSA-Direktor *Alexander* vom 30. Juli 2013, MAT A BND-1/9c, Bl. 243-245 (VS-NfD).

dem „[redacted]“.[742] Präsident *Schindler* stellte durchaus die richtigen Fragen. Jedoch leider erst im Spätsommer 2013.

gg) Die BND-Kanzleramts-Lösung: Anpassung des Rechts an die rechtswidrige Praxis

Die Antwort, die der BND-Präsident vom NSA-Direktor erhielt, sollte den BND und die Bundesregierung zwar in Sachen Überwachung durch die NSA in Deutschland entlasten – die 580 Millionen Daten pro Monat aus BOUNDLESS INFORMANT stammten nach Angaben der NSA aus Bad Aibling und aus der Erfassung des BND in Afghanistan. Diese Erklärung nahm die Bundesregierung dankbar auf. Es tat sich dadurch aber ein neues Problem auf und löste im BND rege Betriebsamkeit aus. Wie konnte der BND erklären, dass er selbst massenhaft Metadaten in dieser Größenordnung erhebt und an die NSA übermittelt? Und wieso waren weder die Fachaufsicht im Kanzleramt noch das Parlament darüber jemals informiert worden?

Vor dem Hintergrund, dass das Kanzleramt dringlich forderte, die Rechtsgrundlage und Rechtsbewertung für eine solche massenhafte Datenübermittlung darzulegen, fühlte sich die BND-Spitze genötigt, die Rechtsgrundlagen für den BND bei der Datenübermittlung an die NSA schnellstmöglich neu zu bewerten. Der BND hatte zu diesem Zeitpunkt im August 2013 wohl selbst feststellen müssen, dass er sich über Jahre hinweg im rechtswidrigen Raum bewegt hatte und rechtswidrig Daten übermittelte, indem er die Übermittlungsvorschriften und Bestimmungen des BNDG und BVerfSchG umging.

Problematisch schien vor allem, dass auch das Kanzleramt sowie die Öffentlichkeit nun davon erfuhren. Es bleibt fraglich, weshalb die Fachaufsicht und hier vor allem die Rechtsaufsicht über den BND im Kanzleramt erst in Folge der Berichterstattung nach

742) Schreiben von Präsident *Schindler* an NSA-Direktor *Alexander* vom 30. Juli 2013, MAT A BND-1/9c, Bl. 243-245 (VS-NfD).

den *Snowden*-Enthüllungen auf die Idee kam, nach einer Rechtsgrundlage für die Abhör- und Übermittlungspraxis zu fragen.[743]

In großer Eile – am Wochenende vor dem 5. August 2013 – verständigte sich BND-Präsident *Schindler* mit seinem Leitungsstab auf eine rechtliche Argumentationslinie,[744] die dann mit dem Abteilungsleiter 6 im Kanzleramt, *Heiß*, abgestimmt wurde. Dabei hatten jedoch weder die Spitzen von BND noch Kanzleramt im Sinn, die rechtswidrige Praxis des BND zu beenden. Um diese weiter fortführen zu können, unternahmen sie vielmehr den Versuch, die Praxis der massenhaften Metadatenübermittlung durch abstruseste Auslegungen des geltenden Rechts zu rechtfertigen. Das dahinterstehende Problem war offenkundig: Die Übermittlungsvorschriften hatte der BND bis dato nicht eingehalten und konnte dies angesichts der Masse und Beschaffenheit der übermittelten Metadaten auch gar nicht.

BND und Kanzleramt verfolgten daher bewusst und gewollt das Ziel, die Datenerfassungen in Bad Aibling und damit auch die Übermittlungen des BND aus dem Geltungsbereich des BNDG (insbesondere § 9 BNDG) herauszudefinieren, um sich so von den lästigen Vorschriften zu befreien.[745] Dazu musste auch die seit 1995 gültige und schriftlich vom Kanzleramt verfügte Weisung beseitigt werden, nach der alle Daten, die der BND wo auch immer erfasst hat, gleichsam nach den Übermittlungsvorschriften des BNDG und BVerfSchG zu behandeln seien. Im August 2013 wurde so die Weisungslage der rechtswidrigen Praxis des BND einfach angepasst. Darin liegt gleichsam eine nachträgliche Billigung der rechtswidrigen Praxis durch die Verantwortlichen im Kanzleramt: den Abteilungsleiter 6 *Heiß* und den Chef des Kanzleramtes *Pofalla*. Sie ist aktenkundig in der von *Heiß* gefertigten Vorlage für den Chef des Kanzleramtes vom 7. August 2013, die *Pofalla* am selben Tag mit seiner Paraphe zustimmend abzeichnete.[746]

---

743) Vgl. *Polzin*, Protokoll-Nr. 72 I, S. 140.

744) BND-interne E-Mail vom 5. August 2013, MAT A BND-40a, Bl. 99 f. (VS-NfD).

745) Vgl. MAT A BND-40a, Bl. 74, 120 (VS-NfD).

746) Vorlage von AL6 *Heiß* für ChefBK *Pofalla* vom 7. August 2013, Betr. „Rechtsgrundlage zur Übermittlung von im Ausland gewonnener Daten an ausländische öffentliche Stellen“, MAT A BK-1/6b, Bl. 76-78 (VS-NfD).

Als Entscheidungsgrundlage diente ein zwei Tage zuvor im BND erstelltes Kurzgutachten[747] mit der von Schindler und Heiß vorgegebenen Linie: 1. Die Metadaten seien im Ausland und damit außerhalb des Geltungsbereiches des BNDG erhoben worden und deshalb vogelfrei („Weltraumtheorie“). Und 2. als Hilfsüberlegung: Metadaten von Ausländern im Ausland seien keine personenbezogenen Daten.[748]

Im Kurzgutachten wird noch eine weitere Hilfserwägung getroffen: Selbst wenn die beiden ersten Auffassungen nicht trügen, würde der BND die Übermittlungsvorschriften aus dem BVerfSchG dennoch einhalten (können). Dies wird jedoch nur um den Preis abgesenkter Anforderungen erreicht, für die es aus unserer Sicht und wie dargelegt keine Rechtfertigung gibt (siehe insb. V.9.a)bb) – Metadaten besitzen eine hohe Aussagekraft).

Der Versuch, diese BND-Argumentation als tatsächlich gangbare Rechtsauffassung zu verkaufen, wird auch im Hinblick auf den Bericht der „Vertrauenperson“ *Graulich* über die NSA-Selektoren deutlich, indem weite Teile des Kurzgutachtens – unreflektiert und wörtlich – Einzug fanden.[749]

aaa) Versuch Nr. 1: Weltraumtheorie

Auch die BfDI-Zeugin *Löwnau* erklärte sich den Grund, warum der BND die Weltraumtheorie erfand, damit „wahrscheinlich, weil man gemerkt hat, man hat dort bestimmte Voraussetzungen nicht erfüllt“.[750] Um dem deutschen Recht zu entkommen, hob der BND gewissermaßen bis in den Weltraum ab.

(1) Der BND sieht sich nicht an deutsches Recht gebunden

Nach der im Kurzgutachten vertretenen Auffassung soll die Datenerhebung des BND nicht auf deutschem Boden stattfinden, sondern direkt an den Satelliten, die sich im Weltraum befinden. Die Satellitenempfangsanlagen in Bad Aibling würden die Daten lediglich von „ausländischen Satelliten“ abgreifen und daher eine Datenerhebung im

---

747) Kurzgutachten des BND vom 5. August 2013, MAT A BK-1/6b, Bl. 65-68 (VS-NfD).

748) BND-interne E-Mail vom 5. August 2013, MAT A BND-40a, Bl. 99 f. (VS-NfD).

749) *Graulich*, MAT A SV-11/2, bspw. S. 62 ff., 90.

750) *Löwnau*, Protokoll-Nr. 72 I, S. 42.

Ausland darstellen. Für die darüberhinaus aus Richtfunkstrecken sowie einer Satellitenempfangsanlage in Afghanistan stammenden Metadaten, die ebenfalls an die NSA übermittelt werden, gelte dies ohnehin. Die Datenerhebungen würden ausschließlich an ausländischen Lebenssachverhalten ansetzen und wären damit definitorisch ‚[redacted].“ Argumentiert wird weiterhin damit, dass es dem Gesetzgeber aufgrund des völkerrechtlichen Souveränitätsprinzips verwehrt gewesen sei, ‚[redacted][751]

Da die Daten nach Auffassung des BND außerhalb des Geltungsbereichs des BNDG erhoben würden, fänden in der Konsequenz auch die Übermittlungsvorschriften i. S. d. § 9 BNDG keine Anwendung mehr.

Nach Interpretation dieser Rechtsauffassung durch die BND-Datenschutzbeauftragte, die Zeugin *Dr. H. F.* – die diese Auffassung vollständig ablehnt –, befände sich der BND nicht nur außerhalb des BND-Gesetzes, „sondern insgesamt außerhalb des deutschen Rechtes, damit auch außerhalb des Bundesdatenschutzgesetzes.“[752] Damit führten Kanzleramt und BND die von der Bundeskanzlerin im Sommer 2013 wie ein Mantra vorgetragene Aussage „dass auf deutschem Boden deutsches Recht gilt,“[753] komplett ad absurdum. Weiter sagte *Merkel* am 19. Juli 2013 gegenüber der Presse:

> „Meine Aufgabe besteht darin, dafür zu sorgen, dass die Bürgerinnen und Bürger in Deutschland wissen: Auf deutschem Boden wird deutsches Recht angewandt, und das gilt für alle, die sich hier aufhalten. Das ist meine Aufgabe.“[754]

---

751) Kurzgutachten des BND vom 5. August 2013, MAT A BK-1/6b, Bl. 65-68 (VS-NfD).

752) *H. F.*, Protokoll-Nr. 16 I, S. 55.

753) Mitschrift der Sommerpressekonferenz von Bundeskanzlerin *Merkel* vom 19. Juli 2013, https://www.bundesregierung.de/ContentArchiv/DE/Archiv17/Mitschrift/Pressekonferenzen/2013/07/2013-07-19-merkel-bpk.html, abgerufen am 18. Juni 2017

754) Mitschrift der Sommerpressekonferenz von Bundeskanzlerin *Merkel* vom 19. Juli 2013, https://www.bundesregierung.de/ContentArchiv/DE/Archiv17/Mitschrift/Pressekonferenzen/2013/07/2013-07-19-merkel-bpk.html, abgerufen am 18. Juni 2017.

Der Chef des Bundeskanzleramtes *Pofalla* sah dies im Hinblick auf den eigenen Auslandsnachrichtendienst offenbar anders. Dass die Diskussionen um die Rechtfertigung der Massendatenübermittlungen komplett an der Bundeskanzlerin vorbeigingen, ist kaum vorstellbar.

(2) Widerstand bei BND-Datenschutzbeauftragter und im Kanzleramt

Die BND-interne Datenschutzbeauftragte *Dr. H. F.* teilte die Auffassung im Kurzgutachten nicht und erhob intern Widerstand. Ihre Äußerungen, sie könne diese Bewertung nicht mittragen[755] wurden letztlich übergangen. Sie wurde vom Justiziar und der BND-Leitung überstimmt.

Auch im Kanzleramt hatte sich Protest gegen diese Neuauslegung erhoben. Bereits am 5. August 2013 wurde eine Vorlage mit der gegensätzlichen Rechtsauffassung des Fachreferats 601 an den damaligen Chef des Kanzleramtes, *Pofalla*, auf den Weg gegeben.[756] Sie verwies auf die zum damaligen Zeitpunkt gültige Weisung des Kanzleramtes von 1995, nach der bei Übermittlungen alle Daten, unabhängig vom Erhebungsort – ob Ausland oder Inland – stets nach den §§ 9, 10 BNDG zu behandeln seien. Auch seien die entsprechenden Verweisungen auf die Übermittlungsvorschriften im BVerfSchG zu beachten.[757]

Diese Vorlage – adressiert an den Chef des Kanzleramtes – wurde nicht weitergeleitet, sondern durch eine neue, vom Abteilungsleiter 6, *Günter Heiß,* persönlich unterzeichnete Vorlage am 7. August 2013 ersetzt. Diese spiegelte die Auffassung des BND-Kurzgutachtens wieder, schloss eine Anwendung des BNDG aus und verwarf gleichzeitig die Weisung von 1995.[758]

---

755) Besprechungsnotiz über ein Telefonat zwischen Fr. *J* vom BND und Herrn *Wolff* vom BKAmt am 5. August 2013, MAT A BND-40a, Bl. 133 (VS-NfD).

756) Vorlage für ChefBK von Referat 601 vom 5. August 2013, MAT A BK-1/6b, Bl. 39 f. (VS-NfD).

757) Grundsätze zur Anwendung des Bundesnachrichtendienstgesetzes (BNDG), Stand: Juli 1995 – Auszug, MAT A BK-1/6b, Bl. 46 f. (VS-NfD).

758) Vorlage von AL6 *Heiß* für ChefBK *Pofalla* vom 7. August 2013, Betr. „Rechtsgrundlage zur Übermittlung von im Ausland gewonnener Daten an ausländische öffentliche Stellen“, MAT A BK-1/6b, Bl. 76-78 (VS-NfD).

Als das abschließend erstellte Kurzgutachten des BND im Rechtsreferat des Kanzleramtes – das die Rechtsmeinung nicht mittrug[759] – einging, wurde sofort erneut unter der Leitung der Zeugin *Polzin*, eine Bewertung verfasst, die die Argumentationslinien im Kurzgutachten, als rechtlich ‚[redacted] qualifizierte. Es wurde auf die in ‚[redacted] für den BND verwiesen.[760] Da jedoch gerade diese beabsichtigt waren, fanden die Bedenken der Mitarbeiter_innen des Rechtsreferates kein Gehör. Die Linie des BND-Präsidenten wurde letztlich auch von der Abteilung 6 und der Leitung des Kanzleramtes mitgetragen.[761]

Die interne Kritik von Mitarbeiter_innen in BND und Kanzleramtes änderte an der Entscheidung für die Aufrechterhaltung der Weltraumtheorie – nach dem Motto „Ober sticht Unter“[762] – nichts. Dass die Leitung des Kanzleramtes nachträglich die rechtswidrige Praxis des BND ebenso wie die künftige billigte, indem sie die Weltraumtheorie absegnete, ist skandalös und ein Rechtsbruch. Die politische Verantwortung tragen vor allem der Chef des Kanzleramtes *Pofalla*, der auch persönlich durch seine Zustimmung verantwortlich ist, und Bundeskanzlerin *Merkel*.

(3) Auffassung des BND rechtlich nicht haltbar

Diese von den Führungsebenen in BND und Kanlzeramt ersonnene Rechtskonstruktion, die allein dem Ziel dienen soll, den Schutz des Grundgesetzes zu umgehen, ist unzulässig und kann keine Überwachungsmaßnahmen tragen. Es handelt sich hierbei, in den Worten des Referatsleiters des Justiziariats des BND, *Ader*, nicht um eine „Theorie im naturwissenschaftlichen Sinne“[763] Führende Rechtswissenschafter_innen se-

759) handschriftlicher Vermerk auf der Unterrichtungsvorlage von AL6 *Heiß* an ChefBK vom 7. August 2013, MAT A BK-1/6b, Bl. 79-81 (79) (VS-NfD),

760) Bewertung Kurzgutachten (BND) zur Weitergabe von Metadaten an AND, MAT A BK-1/6b, Bl. 82-87 (VS-NfD).

761) Vgl. Bundeskanzleramt, Referat 601, Ergebnisprotokoll, Vorbesprechung des Kontrollbesuchs des BfDI in Bad Aibling am 2. und 3. Dezember 2013, MAT A BK-1/6b, Bl. 292 f. (293).

762) Im Fall des „Freibriefs“ aus dem Kanzleramt an die *Telekom* im Rahmen der Operation EIKONAL wurde auf seiten des Betreibers so argumentiert, siehe *Dr. Köbele*, Protokoll-Nr. 33 I, S. 142

763) *Ader*, Protokoll-Nr. 69 I, S. 117.

hen das ähnlich und lehnen sie vehement ab. Nach dem Verfassungsrechtler *Christoph Gusy* handele es sich bei der Weltraumtheorie um „eine Theorie, die von niemandem außerhalb der Nachrichtendienste selbst vertreten wird.“[764]

Die Zeugin *Dr. H. F.* hat vor dem Ausschuss darauf hingewiesen, dass die Rechtsauffassung des Präsidenten aufgrund der Datenbankkonzeption im BND lediglich „im Hinblick auf die Speicherung keine Rolle“ spiele. „Es spielt eine Rolle bei der Frage der Übermittlung. Meiner Rechtsauffassung nach würden die Übermittlungsvorschriften im BND-Gesetz Anwendung finden, nach Rechtsauffassung des Dienstes nicht.“[765]

Verdeutlicht wird hierin die der Weltraumtheorie zugrundeliegenden, irrigen Rechtsauffassungen des BND: dass das Recht der Informationserhebung auch das Recht der Informationsverwendung bestimme. Die Datenübermittlung könne also niemals rechtswidrig sein, wenn durch die Datenerhebung nicht selbst in Grundrechte eingegriffen wurde.[766] Diese Ansicht verfehlt den datenschutzrechtlichen Charakter von Datenübermittlungen. Diese sind zwar von der vorherigen Erfassung abhängig, jedoch rechtlich jeweils als eigenständige Maßnahmen und daher auch als eigenständige Grundrechtseingriffe zu werten. Dies ist insbesondere vor dem Hintergrund relevant, da Übermittlungen ein eigenes, ganz besonderes Gefahrenpotenzial aufweisen. Selbst wenn Daten vom Ausland nach Bad Aibling zugeroutet werden, müssen die Übermittlungsvorschriften für die Weiterleitung an die NSA, mindestens jedoch das BDGS – da es sich um eine Übermittlung auf deutschem Boden und durch eine deutsche Behörde handelt – Beachtung finden.[767]

In der Bewertung des Referats 601 im Kanzleramt zum Kurzgutachten heißt es:

---

764) *Gusy*, Vortrag auf der Fachtagung: Grund- und menschenrechtliche Anforderungen an die Kommunikationsüberwachung des BND am 10. Mai 2016 (mp3, 28 MB) ab Minute 15:15, http://www.institut-fuer-menschenrechte.de/v/338/, zuletzt abgerufen am xxx.

765) *H. F.*, Protokoll-Nr. 16 I, S. 17 f.

766) Vgl. *Gusy*, Vortrag auf der Fachtagung: Grund- und menschenrechtliche Anforderungen an die Kommunikationsüberwachung des BND am 10. Mai 2016 (mp3, 28 MB) ab Minute 15:15, http://www.institut-fuer-menschenrechte.de/v/338/.

767) *Gusy*, Vortrag auf der Fachtagung: Grund- und menschenrechtliche Anforderungen an die Kommunikationsüberwachung des BND am 10. Mai 2016 (mp3, 28 MB) ab Minute 15:15, http://www.institut-fuer-menschenrechte.de/v/338/.

„[redacted]

[redacted]“[768]

Das BVerfG hat in seiner Entscheidung von 1999 ausgeführt, dass ein Bezug bereits bestehe, wenn sich die Empfangsanlagen des Telekommunikationsverkehrs auf deutschem Boden befänden.[769] Dies ist hier der Fall. Die Datenströme werden in der Praxis von der sich auf dem Gelände der Außenstelle Bad Aibling befindenden Satellitenempfangsanlage erhoben.[770] Bad Aibling liegt in Deutschland. Es handelt sich hierbei um eine deutsche Dienststelle mit territorialem Bezug zur Bundesrepublik, die daher dem Geltungsbereich des BNDG unterliegt. Auch stellt der Abgriff in Bad Aibling eine Datenerhebung gem. § 3 Abs. 3 BDSG dar, da der BND hier aufgrund seines aktiven

768) Bewertung Kurzgutachten (BND) zur Weitergabe von Metadaten an AND, MAT A BK-1/6b, Bl. 82-87 (85) (VS-NfD)..

769) BVerfG, 1 BvR 2226/94 vom 14. Juli 1999, Absatz-Nr. 176, http://www.bverfg.de/entscheidungen/rs19990714_1bvr222694.html; vgl. *Bäcker*, http://verfassungsblog.de/der-bnd-baut-sich-einen-rechtsfreien-raum-er-kenntnisse-aus-dem-nsa-untersuchungsausschuss/.

770) Vgl. auch handschriftlicher Vermerk von *H. F.* auf einem Ausdruck des Kurzgutachtens, MAT A BND-40a, Bl. 136 (VS-NfD).

Handelns zumindest die Möglichkeit einer Kenntnisnahme von den Daten erlangt – soweit dies nicht vorher schon geschehen ist – und zudem sogar eine Verfügung über diese begründet.[771] Bei der Verwendung von BND-eigenen Datenleitungen und Datenträgern ist hiervon immer auszugehen. Dass der BND die Metadaten ohne vorherige Einsicht an die NSA übermittelt, ist hier folglich irrelevant, er ist dennoch an das BDSG gebunden.

Auch im Kanzleramt wusste man eigentlich „dass der Datenaustausch (…) auf deutschem Recht basiert.“[772] Es bleibt also die Frage, warum der BND sich nicht „auf deutschem Boden an deutsches Recht“ hielt.

Das Vorgehen des BND verdeutlicht die Relevanz, sowohl inländische und internationale als auch ausländische Telekommunikation rechtlich nach dem Artikel 10-Gesetz zu behandeln.[773] Die hier vorgefundende Strategie des Anpassens der Rechtsinterpretation an rechtswidrige BND-Praxis erinnert an die „Theorie des offenen Himmels“, die von Zeugen im Zusammenhang mit der Operaiton EIKONAL genannt wurde (vgl. Feststellungsteil F.II.4.c)).

An den Vorgängen im Sommer 2013 wird erneut deutlich, dass sowohl BND als auch Kanzleramt nicht daran interessiert waren, die rechtswidrige Praxis an das geltende Recht anzupassen. Vielmehr versuchten sie, wie auch der Obmann der SPD-Fraktion *Christian Flisek* zutreffend in der Vernehmung des Zeugen *Schindler* feststellte, „mit sehr viel Kreativität in der Rechtsauslegung der bestehenden Gesetze (…), den Spielraum des BND durch Aushebelung geltenden deutschen Rechts massiv zu erweitern. Und das ist kein Einzelfall; das zieht sich wie eine rote Linie durch viele, viele Problembereiche, die wir hier vorfinden“.[774] In der Bewertung der Mehrheit (Dritter Teil des Berichts) liest sich das im Ergebnis jedoch völlig anders.

771) Vgl. *Damman*, in: *Simitis*, Kommentar zum BDSG, § 3, Rn. 102.

772) Bundeskanzleramt, Referat 601, Ergebnisprotokoll, Vorbesprechung des Kontrollbesuchs des BfDI in Bad Aibling am 2. und 3. Dezember 2013, MAT A BK-1/6b, Bl. 292 f. (293).

773) Vgl. auch *Christoph Gusy*, Vortrag auf der Fachtagung: Grund- und menschenrechtliche Anforderungen an die Kommunikationsüberwachung des BND am 10. Mai 2016 (mp3, 28 MB) ab Minute 25:50, http://www.institut-fuer-menschenrechte.de/v/338/.

774) Abgeordneter *Flisek*, Protokoll-Nr. 54 I, S. 8 f.

bbb) Versuch Nr. 2: Umetikettierung der Metadaten

Nach Auffassung des BND sind „[redacted] mehr.[775] Begründet wird dies mit dem Argument, dass eine Bestimmbarkeit des Personenbezugs dann nicht gegeben sei, wenn die Person nur mit unverhältnismäßigem Aufwand ermittelbar sei. Bei deutschen Telefonnummern oder E-Mail-Adressen sei dies noch der Fall, „[redacted]“[776] – bei Ausländern im Ausland hingegen nicht. Bei ausländischen Anschlusskennungen sei „[redacted]“. So fehle es „[redacted]t.“[777] Damit sei „[redacted], weshalb ein Personenbezug pauschal entfiele.[778]

Zwar gibt der BND an, dass „[redacted])“ besäßen – [redacted]g.“[779]

Diese Rechtsauslegung, die als Auffangargument entwickelt wurde, um BNDG und Datenschutzgesetz zu entgehen, ist rechtlich nicht haltbar. Selbst intern stieß sie auf erheblichen Widerstand, so auch im Kanzleramt. Hier äußerte die damalige Referatsleiterin 601, die Zeugin *Polzin*, in der Bewertung zum Kurzgutachten des BND, dass die „[redacted]

775) BND-interne E-Mail von *U. K.* (Leitungsstab),vom 5. August 2013, MAT A BND-40a, Bl. 99 (VS-NfD).

776) MAT A BND-40a, Bl. 90 (VS-NfD).

777) Vgl. BND-interne E-Mail von *M. F.*, MAT A BND-40a, Bl. 89 f. (90) (VS-NfD).

778) BND-interne E-Mail von *U. K.* (Leitungsstab),vom 5. August 2013, MAT A BND-40a, Bl. 99 f. (100) (VS-NfD).

779) BND-interne E-Mail eines Sachgebietsleiters aus Bad Aibling vom 5. August 2013 MAT A BND-40a, Bl. 111 f. (VS-NfD).

[redacted]“[780]

Der Anwendungsbereich ist bereits eröffnet, sobald ein Personenbezug unter vernünftigen ökonomischen Aufwendungen herstellbar wäre. „Der Grad der Schwierigkeit eines solchen Identifizierungsverfahrens ist dabei unerheblich, sofern die speichernde Stelle in der Lage ist, mit angemessenem Aufwand eine Beziehung zu dem Betroffenen herzustellen.“[781] Dabei muss auch die Möglichkeit der Zuhilfenahme weiterer verfügbarer Erkenntnisse Dritter, wie der NSA, bei der Zuordnung des Personenbezugs in Betracht gezogen werden.[782]

Vor dem Hintergrund der Methoden und der Technik der US-Dienste und der auf einem Tauschgeschäft fundierenden Kooperation, hätte der BND erkennen müssen, dass ein Ausschluss des Personenbezugs nicht gegeben ist. Dies verdeutlichte der frühere BfDI, *Peter Schaar*, wie folgt:

> „[Werden] Metadaten, die man selber nicht zuordnen kann, an jemanden weiter[geleitet], der sie zuordnen kann, dann wäre es natürlich absurd, wenn man diese Daten aus dem Schutz herausnehmen würde. Wir wissen, dass die NSA in der Lage ist, durch sehr umfassende Verzeichnisdienste Metadaten zuzuordnen. Das ist ja eines der Programme auch, das von der NSA betrieben wird – ich kann mir vorstellen, dass es andere auch gibt –, im Grunde so eine Art Directory zu haben, wo dann die Zuordnung erleichtert wird und gegebenenfalls automatisiert stattfindet, ein System, über das vermutlich deutsche Dienste nicht annähernd irgendwie verfügen. So kann es schon sein, dass Daten, wenn sie denn weitergegeben werden, zum Beispiel Metadaten, die aus dem Ausland stammen, vom BND nicht personenbezogen zugeordnet werden könnten, von dem Empfänger aber doch.

---

780) Bewertung Kurzgutachten (BND) zur Weitergabe von Metadaten an AND, MAT A BK-1/6b, Bl. 82-87 (87) (VS-NfD).

781) Erbs/Kohlhaas/Ambs, BDSG § 3 Rn. 3, https://beck-online.beck.de/?vpath=bibdata/komm/ErbsKoStrafRNebG_213/BDSG/cont/ErbsKoStrafRNebG.BDSG.p3.gl1.htm, abgerufen am 18. Juni 2017.

782) BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015, 1, A, I, 1, a, aa), https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/.

> Also insofern würde ich sagen, Metadaten gehören im Regelfall dazu. Wir haben in der Datenschutzdebatte immer wieder das Thema IP-Adressen gehabt. Da ist es ja noch mal ein bisschen komplizierter. Das sind ja auch Daten, die in den Metadaten häufig mit drinstecken. Aber auch dort muss man sagen, dass letztlich die Zuordnung möglich ist, in vielen Fällen jedenfalls, nicht immer. Und deshalb ist die Regelvermutung: Ja, es sind auch personenbezogene Daten.“[783]

Dass auch IP-Adressen aus den Auslandsverkehren an die NSA ausgeleitet wurden, hat der Zeuge *Breitfelder* bestätigt.[784]

Der G 10-Beauftragte des BND, *A. F.*, räumte in der Ausschusssitzung ein: „Also mit entsprechendem Zusatzwissen ist natürlich jedes dieser Daten bestimmbar.“[785] Dass auch der BND in einigen Fällen Zusatzwissen zu einem Teil der Daten in Form von Telefonnummern oder E-Mail-Adressen besitzt, ist unbestreitbar[786] und deren Sammlung ist Zweck der vom BND betriebenen Datenbanken. Ganz genauso wird es sich nach der bekanntgewordenen Praxis der unzähligen NSA-Datenbanken bei den US-Diensten verhalten.

b) Rechtswidrige Übermittlung von Inhaltsdaten an die NSA

Der BND übermittelte der NSA nicht nur ausgewählte einzelne Informationen wie „Meldungen“, sondern ausnahmslos alle „G-10 bereinigten“ Treffer in Form von Rohmaterial und Finished Intelligence,[787] die mittels der von der NSA übermittelten Selektoren erzielt wurden. Da bereits die Datenerfassung sowie die Selektion mittels der verschiedenen Suchbegriffe und die anschließende Speicherung und Weiterverareitung an sich teilweise gegen deutsches Recht verstießen – insbesondere da es keine Rechtsgrundlage hierfür gab – hätte der BND die Daten zum großen Teil nicht weiterleiten

---

783) *Schaar*, Protokoll-Nr. 31 I, S. 24.

784) *Breitfelder*, Protokoll-Nr. 28 I, S. 68.

785) *A. F.*, Protokoll-Nr. 41 I, S. 118.

786) Vgl. auch handschriftlicher Vermerk von *H. F.*, MAT A BND-40a, Bl. 137 (VS-NfD).

787) E-Mail von *A. F.* an *H. F.*, MAT A BND-40a, Bl. 139 (VS-NfD).

dürfen.[788] Der BND wäre vor diesem Hintergrund in besonderem Maße angehalten gewesen, die Datenübermittlungen stärker zu regulieren und zu kontrollieren. Dem kam der BND nicht nach, er übermittelte massenhaft und anlasslos Daten, ohne die hinreichende Prüfung der Erforderlichkeit der Übermittlung für seine Aufgabenerfüllung gewährleisten zu können. Selbst wenn diese Daten zum Vorteil beider Nationen gewesen wären,[789] fehlte es an einer Rechtfertigungsgrundlage für die massenhaften Grundrechtseingriffe. Auch kann ein Tauschgeschäft mit der NSA auf Basis des MoAs keine Erforderlichkeitsprüfung ersetzen. Es handelt sich hier um schwerwiegende Verstöße der gesetzlichen Übermittlungsvorschriften aus dem BNDG und BVerfSchG.

„Zu diesem Ergebnis gelangt man auch, wenn man unterstellt, dass die von der NSA übermittelten Selektoren ausnahmslos für die Aufgabenerfüllung des BND erforderlich sind und das DAFIS-Filtersystem keine systemischen Defizite aufweist,“[790] so die BfDI in ihrer rechtlichen Bewertung der datenschutzrechtlichen Kontrolle des BND in Bad Aibling.

aa) Viele Datenübermittlungen, wenig Dokumentation

Angaben zum Umfang der Übermittlungen von Telekommunikationsinhalten aus Bad Aibling an die NSA liegen dem Ausschuss für den Zeitraum Oktober 2013 bis März 2014 nur in statistischer Aufbereitung und geheim eingestuft vor.[791]

Für vorangegangene Zeiträume gibt es offenbar derartige Aufstellungen nicht. Denn der BND protokollierte solche Übermittlungen nicht, bevor im Sommer 2013 öffentlich wurde, dass der BND massenhaft Daten an die NSA übermittelt.

Der Referatsleiter T2A, Herr *H. K.*, erklärte vor dem Untersuchungsausschuss:

---

788) Vgl. BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015, G), https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/.

789) Vgl. *T. B.*, Protokoll-Nr. 20 I, S. 40.

790) BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015, G., https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/.

791) MAT A BND-54 (Tgb.-Nr. 235/16 – GEHEIM), Ordner 457, Bl. 1-6.

> „Grundsätzlich ist es so, dass wir die einzelnen übergebenen Daten nicht dokumentieren (…) Wir wissen, wo es herkommt, aber es wird nicht separat dokumentiert.“[792]

Zudem erklärte er, der BND wisse nicht, wie viele Daten übermittelt wurden. Es handelt sich bei der hier in Rede stehenden Übermittlung eben auch nicht mehr um einzelne wenige Daten. Es handelt sich hier klar um einen Verstoß gegen §§ 9 Abs. 2 BNDG i.V.m. 19 Abs. 3 S. 3 BVerfSchG. Das rechtwidrige Verhalten wird durch die fehlende Dokumentation verschleiert. Eine vollständige Aufklärung und eine datenschutzrechtliche Kontrolle wurden verhindert.

Aufgrund der massenhaften Anzahl von NSA-Selektoren ist jedoch davon auszugehen, dass auch die daraufhin ausgeleiteten und vorgehaltenen Treffer-Daten massenhaft vorliegen. Der BND-Mitarbeiter *T. B.* erklärte, dass die Selektoren „zwei-, drei-, viermal am Tag“[793] von den amerikanischen Servern aktiv abgeholt und nach automatisierter G 10-Prüfung ohne hinreichende Einzelfallprüfung in die Erfassungssysteme eingestellt werden. Nach Zeugenaussagen setzte der BND dabei rund 14 Millionen Selektoren für die NSA ein, mit denen er die erfassten Datenströme durchsuchte, um die damit erzielten Treffer samt der damit zusammenhängenden Metadaten direkt an die NSA zu übermitteln.[794] Treffer von IP-Verkehren sind dabei im Millionenbereich übermittelt worden.[795]

bb) Unzureichende Erforderlichkeitsprüfung

Die Übermittlung ausgefilterter personenbezogener Daten wäre – wie auch bei den Metadatenübermittlungen – zudem nur gemäß den Vorgaben der § 9 Abs. 2 BNDG i. V. m. § 19 Abs. 3 BVerfSchG zulässig gewesen. (vgl. oben Kapitel V.9.a)ff)) Der BND hat jedoch nicht in ausreichendem Maße geprüft, ob die jeweiligen Datenübermittlungen der Inhaltsdaten zur Erfüllung seiner Aufgaben erforderlich waren. Insbesondere

792) *H. K.*, Protokoll-Nr. 81 I, S. 9.

793) *T. B.*, Protokoll-Nr. 20 I, S. 29.

794) *W. K.*, Protokoll-Nr. 118 I, S. 22f.

795) *Löwnau*, Protokoll-Nr. 72 I, S. 32.

fanden hierfür keine qualifizierten Einzelfallprüfungen statt. Eine generelle, d. h. ausnahmslose Übermittlung ist mit dieser gesetzlichen Vorgabe nicht zu vereinbaren. Vor allem berief sich der BND auf die vorherige Überprüfung der NSA-Selektoren.[796] Diese war jedoch – wie in Kapitel V.8 gezeigt – unzulänglich. Selbst in der Annahme, dass der BND diese vollständig hätte überpüfen können, hätte dies nicht die notwendige separate Überprüfung einer Erforderlichkeit für die Datenübermittlungen der „Treffer" ersetzen können. Problematisch ist vor allem jedoch auch, dass die Daten tatsächlich in der Praxis mittels materiell unzulässiger Selektoren abgegriffen wurden, die zum Teil gegen deutsches Recht und Grundrechte verstießen und daher nie hätten verwendet werden dürfen.

Indem der BND in großem Umfang nicht erforderliche Inhaltsdaten an die NSA übermittelte, griff er in das Fernmeldegeheimnis sowie in Persönlichkeitsrechte und speziellere Grundrechte ein.

aaa) Folgenreicher Einsatz der NSA-Selektoren

Das Fehlen einer Prüfung vor der Übermittlung ist besonders schwerwiegend, da es der BND zeitgleich zuließ, dass der US-amerikanische Nachrichtendienst auf die Erfassungsergebnisse konkreten Einfluss nehmen konnte, indem der BND, die von der NSA gewünschten Suchmerkmale einstellte, und ihr die Ergebnisse weiterleitete.

Die BND-Datenschutzbeauftragte *Dr. H. F.* gestand vor dem Ausschuss ein, „dass der behördliche Datenschutz sich der Abteilung TA insgesamt, damit unter anderem sicherlich auch der Selektorenfrage, hätte intensiver widmen müssen."[797]

Infolge der Verwendung unzulässiger Suchbegriffe ist davon auszugehen, dass der BND auch Telekommunikation erfasst hat, die für seine Aufgabenerfüllung nicht erforderlich, also unzulässig war, und an die NSA übermittelt hat.

796) *H. K.*, Protokoll-Nr. 81 I, S. 8.

797) *H. F.,* Protokoll-Nr. 121 I, S. 14.

Auch die BfDI hat bei ihrer Prüfung im Ergebnis festgestellt: Diese Datenverwendungen sind schwerwiegende Verstöße gegen das BNDG sowie das BVerfSchG.[798]

bbb) Automatisiertes Ausleiten rechtswidrig

Der BND hätte vor allem, über die Pflicht der zureichenden Prüfung der NSA-Selektoren hinaus, die aufgrund der Selektoren erzielten Treffer einer eigenständigen Überprüfung der Erfoderlichkeit einer Übermittlung im Einzelfall unterziehen müssen. Die bloße Weiterleitung der Inhalte an sich hat ein enormes eigenständiges Gefahrenpotenzial beinhaltet. Die erzielten Inhaltsdaten können über die Angaben in den Selektoren hinaus weitere konkrete, besonders schützenswerte Informationen und Details beinhalten. Auch lassen sich die Inhaltssuchbegriffe der NSA unbegrenzt kombinieren und verknüpfen.[799] Daraus können eine Unmenge an Ergebnissen erzielt werden, die gerade nicht schon durch den Selektor vorhersehbar sind. Diese neue besondere Qualität muss insbesondere in der Übermittlung Beachtung finden. Die Inhalte müssen daher im Einzelfall und mit besonderer Sorgfalt überprüft werden.

Doch der BND nahm, wenn überhaupt, nur eine stichprobenhafte händische Überprüfung vor. Ob eine Überprüfung bei einer automatischen Weiterleitung dieser Datenmengen überhaupt möglich ist, bleibt fraglich. Nach eigenen Angaben war der BND bereits mit den Treffern seiner eigenen Selektoren schon so „überlastet“, dass eine Überprüfung der aufgrund von NSA-Selektoren erzeugten Meldungen nicht vorgenommen werden konnte.[800] So erklärte der Zeuge *R. U.* vor dem Ausschuss:

> „Man hat die Meldungen, also die Treffer, nur stichprobenartig ausgewertet. Und immer nur dann, wenn bei uns die Notwendigkeit dafür da war, sprich, wenn bei uns zum Beispiel in einem Krisengebiet, in einem Zielgebiet wir zu wenige BND-eigene Selektoren hatten, dann

798) Vgl. BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015, https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/.

799) Vgl. BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015, 1, D, I), https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/.

800) *R. U.*, Protokoll-Nr. 47 I, S. 22 f.

> haben wir da draufgeguckt. Aber es gab keinen Regelautomatismus, keine bestimmten Abstände“.[801]

Auch aufgrund der fehlenden Möglichkeit zur Herstellung der Lesbarkeit konnte eine Durchsicht aller Inhalte nicht stattfinden. Dies wird besonders erheblich, da der BND zum Teil nicht überblicken konnte, nach welchen Daten die NSA suchte. In einigen Fällen waren bereits die NSA-Selektoren für die BND-Mitarbeiter_innen nicht lesbar. Auch eine Deutung bzw. Begründung der NSA für den Einsatz des jeweiligen Selektors fehlte in den meisten Fällen bzw. war nicht lesbar, wodurch eine Überprüfung der Selektoren teilweise von vornherein ausgeschlossen war. Das gegenseitige – und unseren Ergebnissen nach nicht gerechtfertigte – Vertrauen der Geheimdienste auf die Rechtmäßigkeit der eingesetzten Selektoren kann eine Überprüfung der ausgeleiteten Daten nicht ersetzen. Im Ergebnis wusste der BND nicht, welche Daten er an die NSA übermittelte. Dies ist als klarer Rechtsverstoß zu werten.

Weiterhin besteht die Möglichkeit, dass andere Ergebnisse erzielt werden, die mit dem ursprünglichen Suchbegriff in nur geringem oder auch keinem tatsächlichen Zusammenhang stehen und lediglich als „Beifang“ mitausgeleitet wurden. Dem hätte der BND bereits im Vorfeld eine vollständige und einzelfallbezogene Erforderlichkeitsprüfung der übermittelten Inhalte entgegenhalten müssen.[802]

cc) Mangelnde Zweckgebundenheit

Die übermittelten Informationen waren zudem nicht ausreichend zweckgebunden. Da der BND häufig nicht wusste, was er übermittelte, konnte er den Zweck nicht weiter konkretisieren. Im Schriftverkehr verwendet der BND routinemäßig einen „Disclaimer“, der die Nutzung der übermittelten Daten allgemein auf nachrichtendienstliche Zwecke beschränkte und bestimmte Verwendungen untersagte.

---

801) *R. U.*, Protokoll-Nr. 47 I, S. 22.

802) BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015, https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/.

Ob ein Disclaimer bei automatisierten Übermittlungen von Inhaltsdaten verwendet wurde, ist zu bezweifeln. Bei Metadatenübermittlungen haben dies BND-Zeugen ausdrücklich ausgeschlossen mit dem Hinweis, die Daten müsste man ja sonst ausdrucken. Dies gilt selbstverständlich auch für die millionenfache Übermittlung der „Treffer“. Ohnehin kann ein solcher „Disclaimer“ zweifelsfrei keine Zweckbindung begründen. Ein solch pauschaler „Disclaimer“ hebt vor allem nicht die Verantwortung des BND auf, die Verwendung der übermittelten Daten auch zu überprüfen und stets einzufordern.

10. Behinderung der Bundesbeauftragten für den Datenschutz

a) Behinderungen durch das Bundeskanzleramt

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) hat im Verlauf der *Snowden*-Enthüllungen umfangreiche Bemühungen zur Aufklärung möglicher missbräuchlicher Datenverarbeitungen durch bundesdeutsche Geheimdienste entfaltet. Dabei ist sie mehrfach wiederholt und massiv insbesondere durch das Bundeskanzleramt bei der ihr nach dem Gesetz zugewiesenen Aufgabe der Kontrolle der Geheimdienste behindert worden.

Die BfDI zählt, neben anderen Institutionen, zu den verantwortlichen Aufsichtsbehörden der Geheimdienste in der Bundesrepublik. Ihr ist gemäß § 24 Bundesdatenschutzgesetz die Aufgabe zugewiesen, die Beachtung der Einhaltung von allgemeinen und bereichsspezifischen, für BND und BfV geltenden Datenschutzregelungen zu überwachen und zu kontrollieren. Den BND trifft dementsprechend eine korrespondierende Mitwirkungspflicht nach § 24 Abs. 4 S. 1 BND-Gesetz in Verbindung mit § 11 BND-Gesetz (Rechtslage während des UA-relevanten Überprüfungszeitraums). Die allgemeine und umfassende Pflicht des BND, die BfDI bei der Erfüllung ihrer Aufgaben zu unterstützen, wird konkret ergänzt durch ein Auskunftsrecht, ein Einsichtsrecht sowie Zutrittsrechte zu allen Diensträumen.[803]

In Wahrnehmung der ihr von Verfassung wegen zugewiesenen Kontrollaufgaben griff der damalige Bundesbeauftragte *Peter Schaar* die im Juni 2013 beginnende Berichterstattung über die *Snowden*-Enthüllungen auf: mit Schreiben vom 5. Juli, 23. Juli, 27.

803) Unbestritten, vgl. nur *Gola/Schomerus*, 12. Auflage, 2015, § 24, Rdnr. 12.

Juli, 8. August 2013 wandte er sich an das Bundeskanzleramt mit einer Reihe von konkreten Nachfragen zur Berichterstattung und dem dazu möglicherweise vorhandenen Wissen der Bundesregierung. Diese Fragen blieben im Wesentlichen, trotz großzügiger und nicht unüblicher Fristen über Monate unbeantwortet. Sie mündeten schließlich in den Kontrollbesuchen der BfDI am 2./.3. Dezember 2013 in der Außenstelle des BND in Bad Aibling.

Die dem Ausschuss übergebenen Akten belegen Kanzleramts-interne Diskussionen um die Vorgehensweise bei der Beantwortung der mit Fristen versehenen Anfragen bereits zu Anfang August 2013. Während die zuständig befasste Mitarbeiterin, unter Verweis auf eine drohende Prüfung durch die BfDI in der Außenstelle Aibling und wegen möglicher negativer Reaktionen in der Presse eine fristgerechte Beantwortung vorschlug, wiesen der Abteilungsleiter 6 *Heiß* und sein Stellvertreter *Schäper* die Mitarbeiterin an, die zunächst großzügig gesetzte Frist von einem Monat verstreichen zu lassen. Auch die im zweiten Schreiben der BfDI vom 23. Juli gesetzte zweiwöchige Frist wurde nicht eingehalten und schließlich eine einmonatige Fristverlängerung erbeten.

Begründet wurde die Notwendigkeit der Fristverlängerung intern mit eigenen Aufklärungsbemühungen. So hatten u. a. Nachfragen des Bundeskanzleramtes beim BND nicht vertretbare Rechtspositionen wie die Weltraumtheorie zutage gefördert, die von der Arbeitsebene der mit der Fachaufsicht betrauten Abteilung im BKAmt offenbar erstmalig überhaupt wahrgenommen und nicht geteilt wurden. In einer Vorlage für den Chef des Kanzleramtes, *Pofalla*, vom 13. August 2013 wurden jedoch bereits intensiv die rechtlichen Strategien für den Fall einer möglichen Prüfung der BfDI in Bad Aibling erörtert.[804] Man verlegte sich damit frühzeitig, entgegen der Auskunftspflicht, auf eine weitgehende Nichtbeantwortung der Fragen der BfDI und bereitete sich stattdessen intensiv auf eine Vor-Ort- Prüfung der BfDI in Bad Aibling vor.

Die Aktenlage sowie die damit übereinstimmenden Zeugenaussagen belegen damit ganz eindeutig, dass das Bundeskanzleramt wiederholt gegen seine Mitwirkungspflicht gegenüber der BfDI verstoßen hat. Die Akten offenbaren insoweit eine in der

804) ChefBK-Vorlage von Referat 601 vom 13. August, MAT A BK-1/6b, Bl. 130-132.

zuständigen Abteilung 6 zunächst bestehende, völlige Unkenntnis der Vorgänge und Arbeitsweisen in Bad Aibling. Wohl deshalb konnten schon einfache Nachfragen der BfDI nach den Rechtsgrundlagen für die dort vorgenommenen Datenverarbeitungen nicht beantwortet werden. Stattdessen begann in Vorbereitung eines möglichen Prüftermins der BfDI eine kontroverse interne Debatte um die rechtliche Einordnung einiger Praktiken von BND und NSA in Bad Aibling. Dabei übernahm das Bundeskanzleramt schließlich die zunächst von der eigenen Fachaufsicht in mehrerlei Hinsicht als für abwegig befundene Rechtsauffassung des BND, darunter u.a. die sog. Weltraumtheorie[805]

Neben diesen Behinderungen wurde die Aufsichtstätigkeit der BfDI auch bei der im Dezember 2013 stattgefundenen Prüfung selbst konkret behindert.

b) Behinderungen durch den BND bei der Kontrolle in Bad Aibling

Sowohl der BND als auch das Bundeskanzleramt haben die unabhängige Kontrolltätigkeit der Bundesbeauftragten für den Datenschutz (BfDI) wiederholt und massiv behindert. Der BfDI sowie der Datenschutzbeauftragte des BND wurden, als sie u. a. 2013 den Standort in Bad Aibling besuchten, bestimmte Aspekte der massenhaften Datenübermittlung in Bad Aibling an ausländische Nachrichtendienste vorenthalten.[806] Der BND verweigerte Auskünfte bzgl. der Zusammenarbeit und verwehrte den Datenschützer_innen den Zugang zum Verbindungsbüro der SUSLAG.[807]

Insbesondere wurde zunächst die behördliche Datenschutzbeauftragte des BND

, [redacted]

---

805 Vgl. hierzu Kapitel V.9 Datenübermittlung des BND an die NSA aus Bad Aiblingen

806) *Schaar*, Protokoll-Nr. 31 I, S. 10; *H. F.*, Protokoll-Nr. 16 I, S. 42, Vorlage eines internen Vermerks von Dr. *H. F.* v. 20. August 2013 durch die Abgeordnete *Warken*).

807) BfDI, Sachstandsbericht, 1, A, VI), https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/.

> [redacted]“[808]

Im Nachhinein haben die Datenschützer_innen – zunächst des BND selbst und in der Folge auch die BfDI festgestellt, dass der BND die Zusammenarbeit, bezogen auf die Inhaltserfassung schilderte und die Metadatenerfassung schlichtweg nicht thematisierte.[809] Argumentiert wurde dies seitens des BND damit, „dass man das Thema ‚Metadatenanalyse bzw. -erhebung‘ habe zugunsten der Erörterung anderer Themen ausklammern wollen.“[810]

Die BfDI ist jedoch anderer Meinung. Sie hat

> „[redacted][811]

Vor diesem Hintergrund kann es nur verwundern, wenn der BND bzgl. des Themas Datenschutzkontrolle auf die Datenschützer zurück verweist. So sagt der Zeuge *R. U.*:

> „Bei uns in Bad Aibling, (…) werden da gut „betreut“ (…) und beaufsichtigt von unserer eigenen Datenschutzbeauftragten, die bei uns vor Ort sich natürlich alle Systeme intensiv anschaut, die auch dafür Sorge trägt, dass an den Stellen, wo es nötig ist, auch Dateianordnungen erfolgen durch den Bundesnachrichtendienst, und insofern tragen

808) Vermerk der behördlichen Datenschutzbeauftragten des BND, Dr. H. F., vom 20. August 2013, MAT A BND-1/6a, Bl. 239 (VS-NfD).

809) *H. F.*, Protokoll-Nr. 121, S. 19 f.; *R. U.*, Protokoll-Nr. 47 I, S. 22.

810) Vermerk der behördlichen Datenschutzbeauftragten des BND, Dr. H. F., vom 20. August 2013, MAT A BND-1/6a, Bl. 239 (VS-NfD); vgl. *H. F.*, Protokoll-Nr. 16 I, S. 43.

811) Vermerk der behördlichen Datenschutzbeauftragten des BND, Dr. H. F., vom 20. August 2013, MAT A BND-1/6a, Bl. 240 (VS-NfD).

> wir da meiner Meinung nach an jeder Stelle dem deutschen Datenschutz, so gut wir es als Techniker in Zusammenarbeit mit Juristen können, Rechnung.“[812]

Der Kernbereich der Zusammenarbeit, insbesondere der Datenweitergabe an die NSA, blieb somit einer Aufklärung und effizienten datenschutzrechtlichen Kontrolle entzogen. Dieses Verhalten des BND ist auch ein schwerwiegender Verstoß gegen die dem BND obliegende Unterstützungspflicht gemäß § 11 BNDG i. V. m. § 24 Abs. 4 S. 1 BDSG und damit klar rechtswidrig. Es verdeutlicht weiterhin die bisherigen Grenzen der Kontrollmöglichkeiten und -mittel der zuständigen Fachbehörde des Bundes und die damit verbundene dringliche Notwendigkeit zur effektiven Verbesserung dieser. Nicht zuletzt, da nach „Auskunft des BND (…) der Dienst zudem über derart große Datenbestände [verfügt], die – auch unter maximalem Einsatz aller personellen Ressourcen – aufgrund der Masse der Daten nicht in absehbare Zeit entsprechend vorgesichtet bzw. geprüft werden könnten.[813] Diese Beschränkung der Kontrollkompetenz steht im Widerspruch zu den Vorgaben des BVerfG, denn sie stelle einen

> „verfassungswidriger Eingriff in das Grundrecht der Betroffenen auf informationellen Selbstbestimmung“ dar.[814]

Aus dem im Internet abrufbaren abschließenden Prüfbericht der BfDI geht schließlich auch hervor, dass ihr, entgegen ihrer ausdrücklichen Aufforderung, eine Kenntnisnahme der von der NSA zugelieferten, aber auf den IT-Systemen des BND eingespielten Rastermerkmale (sog. US-Selektoren) verweigert wurde. Damit war ihr die letztlich zentrale rechtliche Prüfung nicht möglich, ob die, neben anderen Formen der Datenverarbeitung und Datenübermittlung, stattfindende dauerhafte Rasterfahndung nach

---

812) *R. U.*, Protokoll-Nr. 14 I, S. 60.

813) BfDI, Sachstandsbericht – rechtliche Bewertung, 1, A, I, 3, b, bb, 1), https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/.

814) Sachstandsbericht – rechtliche Bewertung, 1, A, I, 3, b, bb, 1), https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/.

Kommunikationen bestimmter Personen dem datenschutzrechtlichen Erforderlichkeitsprinzip entspricht, welches allgemein als verfassungsrechtlich gebotene Ausprägung des Verhältnismäßigkeitsgrundsatzes angesehen wird.

Ebenfalls verweigert wurde der BfDI der Zutritt zu dem auf dem BND-Gelände in Bad Aibling befindlichen Gebäude (sog. Blechdose oder „Tin Can“), in der nach Aussagen des BND ausschließlich NSA-Bedienstete mit Datenverarbeitungen beschäftigt sind, obwohl es sich dabei um bundesdeutsches Hoheitsgebiet handelt und für das entsprechende Gebäude auch keine anderweitigen rechtlichen Vereinbarungen gelten.

Die für beide Beschränkungen zum damaligen Zeitpunkt angeführten Rechtsauffassungen vertritt die Bundesregierung bis heute und nicht nur das. Sie hat im Nachgang ihre zum damaligen Zeitpunkt zur Verhinderung öffentlicher Aufklärung ad hoc bezogenen Rechtsauffassungen in gesetzliche Positionen umgewandelt. Das Betretungsrecht der BfDI zu Räumen, in denen ganz oder überwiegend Beschäftigte eines ausländischen Nachrichtendienstes mit tätig werden, wurde zuletzt, im Rahmen des sog. Datenschutzumsetzungs- und Anpassungsgesetzes, gesetzlich beschränkt.

Im Ergebnis verweigerte damit die Bundesregierung nachweislich nicht nur im Untersuchungszeitraum, sondern bis heute bewusst und vorsätzlich die Ausübung der nach Auffassung des Bundesverfassungsgerichts (vgl. BVerfG vom 24. April 2013, 1 BVR 1215/07) aus rechtsstaatlichen Erwägungen besonders dringend gebotenen, effektiven Aufsicht der Geheimdienste.

VI. Die Operationen GLO[redacted] und M[redacted]S[redacted]

1. Operation GLO[redacted]

Diese Operation zwischen dem Bundesnachrichtendienst (BND) und einem weiteren amerikanischen Nachrichtendienst erfolgte jenseits einer rechtlichen Rechtfertigung oder Grundlage. Dies ist ein wichtiges Ergebnis der Arbeit des NSA-Untersuchungsausschusses.

In seiner Vernehmung am erklärte der Zeuge *S. L.*, Mitarbeiter der BND und angehört als Projektleiter der Operation EIKONAL[815]:

> „Es gab noch einen weiteren Ansatz, in dem Meldungen an einen AND weitergleitet wurde.“[816]

Näheres dazu berichtete der Zeuge *S. L.* anschließend in eingestufter Sitzung.[817] In Veröffentlichungen der Medien wurde beschrieben, dass der BND sich bei der Firma *MCI Deutschland GmbH* in Hilden Zutritt verschafft habe.[818] Unter der Legende, Techniker im Auftrag des US-amerikanischen Mutterkonzerns *MCI*, (später *Verizon*) zu sein, soll er Telekommunikationsverkehre ausgeleitet, verarbeitet und sowohl selbst genutzt als auch an die CIA (Central Intelligence Agency) als amerikanischen Partner übermittelt haben.[819] Die Operation wurde in den Jahren 2004 bis 2006 durchgeführt.[820]

---

815) Vgl. hierzu Kapitel V. Kooperation des BND mit der NSA: EIKONAL und Bad Aibling.

816) *S. L.*, Protokoll-Nr. 26 I, S. 76.

817) *S. L.*, Protokoll-Nr. 26 II – Auszug offen, S. 12 ff.

818) *Der Spiegel* vom 14. Dezember 2014, „Der BND kooperierte beim Abgreifen von Daten mit der CIA“ und vom 9. Januar 2015 „US-Telefonriese ließ BND mithören“.

819) *Der Spiegel* vom 5. September 2015, „Die Legende von Hilden“; *golem.de* vom 24. Februar 2015 „Operation Glotaic – Der BND griff Daten offenbar über Tarnfirma ab“ https://www.golem.de/news/operation-glotaic-bnd-griff-daten-offenbar-ueber-tarnfirma-ab-1502-112571.html (abgerufen am 16.06.2017).

820) *Spiegel Online* vom 4. September 2015 „CIA hatte direkten Zugriff auf deutsche Telekommunikation“, abrufbar unter http://www.spiegel.de/netzwelt/netzpolitik/cia-hatte-direkten-zugriff-auf-deutsche-telekommunikation-a-1051407.html (abgerufen am 16.06.2017).

Die Vorüberlegungen und erste Gespräche der beteiligten Dienste fanden im Klima der „uneingeschränkten Solidarität“ unmittelbar nach dem 11. September und den beginnenden Kriegen in Afghanistan und dem Irak statt. Dies legt die Vermutung nahe, dass die mehrfach von Zeug_innen beschriebenen Überlegungen und etwaigen Zweifel innerhalb des BND im Ergebnis als hinderlich beiseite gewischt wurden. So schildert auch der Zeuge *W. K.* die Überlegungen zu Beginn der Planungsphase:

> „Wir sahen uns damals, nach 2001 – ich habe schon mal erwähnt: beginnender Afghanistan- Krieg, Beteiligung Deutschlands –, vor der Aufgabe, mehr Ergebnisse zu bringen mit Richtung Terrorismusabwehr und Force Protection, also in Richtung Nah-/Mittelost.“[821]

Der Zugriff auf Telekommunikationsverkehrsdaten in Deutschland bedarf nicht nur einer rechtlichen Grundlage, sondern auch einer richterlichen Genehmigung bzw. durch einer solchen durch ein konzeptionell vergleichbares Gremium.[822] Nach dem Ergebnis der Beweisaufnahme steht fest, dass für den Abgriff dieser Operation keinerlei entsprechende Genehmigung eingeholt wurde oder noch eine solche ergangen ist. Insbesondere wurde auch keine Genehmigung der G 10-Kommission eingeholt.

Da Bestandteile der vom Untersuchungsausschuss beigezogenen Beweismaterialien nach entsprechender Konsultation nicht freigegeben wurden, lässt sich nicht abschießend feststellen, mit welchem Ziel die Operation begründet wurde. Insbesondere das hierzu zwischen den beteiligten Diensten getroffene sog. *Note of Agreement* konnte durch den Ausschuss nicht ausgewertet und bewertet werden. Sämtliche diesbezüglich zum Umfang und Inhalt der Vereinbarung abgegebenen Zeugenaussagen sind im Ergebnis lückenhaft und unvollständig, da auch die Aussagegenehmigung der Zeug_innen entsprechend konkrete Angaben nicht zuließ. Die vage umrissene Zielrichtung („Terrorismusabwehr“, „Force Protection“, „Nah- und Mittelost“) der Operation bewegt sich im öffentlich erklärten Rechtfertigungsrahmen des Aufgabenprofils der Bundesregierung für den BND. Eigene Feststellungen der Erfassungsziele hat der Ausschuss nicht machen können. Erfolgreiche Aufklärungsergebnisse im Sinne des

---

821) *W. K.*, Protokoll-Nr. 35 II – Auszug offen, S. 9.

822) *Papier*, SV-2/2, S. 5 unter Hinweis auf BVerfGE 125, 260 (368), http://www.bverfg.de/e/rs20100302_1bvr025608.html.

Aufgabenprofils bzw. der weit umrissenen Ziele erbrachte die Operation tatsächlich nicht[823]. Die unklare und offenbar ins Blaue hinein geplante und erfolgte Erfassung von Kommunikationsdaten und –inhalten entbehrte tatsächlicher Anhaltspunkte einer konkreten Gefahr für die zu schützenden Rechtsgüter.[824] Die geäußerten Vermutungen – vgl. *W. K.* unter Fußnote 6 – reichen nicht aus.[825]

Auf die eigentlichen Gründe für die Operation lassen die Angaben der Zeug_innen wie folgt schließen. Der Zeuge *W. K.* hat betont, dass es sich um einen langjährigen und engen Partnerdienst des BND handelte. Zudem sei es die erste Operation gewesen, bei welcher für die Datenerfassung und Selektion auch mit Erfassungswünschen des ausländischen Dienstes gearbeitet worden sei. Dies lässt den Schluss zu, dass sowohl im hiesigen Fall der BND auch darauf bedacht war, seinen eigenen Stellenwert sowohl gegenüber der NSA als auch dem anderen amerikanischen Nachrichtendienst zu erhöhen. Dafür spricht, dass der BND seinerseits nicht darauf bestanden hat, den Erfassungsansatz mit einer förmlichen Anordnung zu verwirklichen. Insbesondere vor dem Hintergrund, dass nach Angaben des verantwortlichen Unterabteilungsleiters *W. K.* der Zugriff auf jedenfalls vermeintlich reine Ausland-Ausland-Verkehre immer vom Einverständnis des Telekommunikationsbetreibers, hier der früheren *MCI Deutschland GmbH*, abhängig gewesen wäre. Weil die Telekommunikationsüberwachungsverordnung keine Anwendung fand.[826] An einem Einverständnis des deutschen Tochterunternehmens fehlte es sowohl nach den vorgelegten Unterlagen als auch nach Angaben des Zeugen *Oliver Matt* als Vertreter der *Verizon Deutschland GmbH*. Der Zeuge *Urmann* hat insoweit allgemein gehalten bestätigt, dass bei derlei Operationen immer auch Nebenziele verfolgt werden.

Durchaus als Bedeutungszuwachs dürfte der BND gewertet haben, dass der amerikanische Nachrichtendienst den Erfassungsabgriff gegenüber der US-amerikanischen Konzernmutter des deutschen Tochterunternehmens durchgesetzt und sich dazu eines Schreibens des damaligen BND-Präsidenten *August Hanning* bedient hatte. Der

---

823) *W. K.*, Protokoll-Nr. 35 II – Auszug offen, S. 10.

824) BVerfGE 125, 260 (330), http://www.bverfg.de/e/rs20100302_1bvr025608.html.

825) *Papier*, SV-2/2, S. 4.

826) *W. K.,* Protokoll-Nr. 35 I, S. 16.

damalige BND-Präsident hat die bestimmende Rolle des amerikanischen Nachrichtendienstes so beschrieben:

> „Ich meine, das hat ja im Grunde, wenn ich das alles sehe, die US-Seite alles abgedeckt, also die ganze Willensbildung auf der US-Seite, wer ist da zu beteiligen und wie läuft das und so; das ist doch ganz offenkundig.“[827]

Bedeutsam ist: Entgegen der Darstellung des BND hatte er selbst offenkundig nicht die Leitung der Operation in der Hand inne. Zustandekommen und die fortlaufende Kommunikation mit dem Betreiberunternehmen erledigte der amerikanische Dienst. Der BND war für die technische Umsetzung und Betreuung zuständig bei – ganz wichtig zu betonen – hälftiger Kostenteilung. Die vom Zeugen *W. K.* als bloß mittelbar[828] bezeichnete Beteiligung des amerikanischen Dienstes ist daher eine mindestens beschönigende Darstellung.

Als Rechtfertigungsgrundlage soll für die Operation die Rechtsauffassung des BND herhalten, dass für die Erfassung reiner Ausland-Ausland-Verkehre die Aufgabennorm des § 1 BNDG ausreiche. Diese Auffassung ist nicht haltbar.[829] Im vorliegenden Falle hat der BND selbst bekundet, dass die ausgeleiteten Daten mit einer „G 10“-Filterung und einer Filterung nach US-Bürger_innen verarbeitet wurden.[830] Dies erscheint auch im Hinblick auf die vermeintlich erfolgte „Positivselektion“ im Sinne der reinen Trefferauswahl- und -ausleitung fragwürdig. Dies bedeutet in der Konsequenz, dass dem BND nicht bekannt war, welche Ziele und Interessen vom Partner aufgeklärt werden sollten. Er konnte also nicht sicher sein, dass die Erfassungsziele des Partners sich nicht auf deutsche oder US-Bürger_innen richteten. Die teils erklärte Rechtfertigung, dass die bloß kurzfristige Erfassung von auch nach Auffassung des BND geschützten

827) *Dr. Hanning*, Protokoll-Nr. 65, S. 42.

828) *W. K.*, Protokoll-Nr. 35 I, S. 6.

829) *Bäcker*, SV-2/3, S. 19f.; *Hoffmann-Rhiem*, SV-2/1, S. 11f.; *Papier*, Beschränkungen der Telekommunikationsfreiheit durch den BND an Datenaustauschpunkten, NVwZ–Extra 15/2016, S. 1 ff., abrufbar unter http://rsw.beck.de/rsw/upload/NVwZ/NVwZ-Extra_2016_15.pdf .

830) *W. K.*, Protokoll-Nr. 35 II – Auszug offen, S. 33; *J. F.*, Protokoll-Nr. 35 I, S. 60.

Kommunikationsdaten kein Eingriff in das Fernmeldegeheimnis bedeute, ist angesichts des hier geschilderten Vorgehens unhaltbar. Denn für den erforderlichen Filterungsschritt mussten die erfassten Inhaltsdaten – anderes wurde nicht verarbeitet[831] – inhaltlich verarbeitet und ausgewertet, um die Identität der Kommunikationsteilnehmer festzustellen und den Kernbereichsschutz zu gewährleisten. Die Schizophrenie der Rechtsauffassung des BND wird hier besonders deutlich.

Zudem wurden die erfassten Kommunikationsinhalte auf ihre Relevanz geprüft, also ob sie überhaupt einen nachrichtendienstlichen Wert hatten und somit auch für die Erfassung des BND nutzbar waren. Dass ein solcher Aufwand betrieben wurde, obwohl es sich nur um Telefonie und Fax gehandelt hatte, in deren Erfassung der BND erfahren und erprobt war, muss stutzig machen. Die besondere Betonung der Relevanzprüfung lässt sich nicht nur mit der geschilderten zunächst händischen Prüfung im Probebetrieb erklären, da sie erkennbar nicht auf diesen Operationsabschnitt beschränkt war. Die jahrelange Praxis des BND bei der Überwachung vermeintlich ungeschützter Ausland-Ausland-Verkehre musste in der praktischen Umsetzung immer auch mit einer inhaltlichen Auswertung von Kommunikationsinhalten zur Feststellung der Identität der Kommunikationsteilnehmer_innen und zur Beachtung des Kernbereichsschutzes einhergehen.

Die Operation GLO[redacted] ist nach den Feststellungen des Untersuchungsausschusses ohne jedenfalls formelle Kenntnis des Bundeskanzleramtes als zuständiger Fachaufsicht und auch ohne Kenntnis des Bundesinnenministeriums – welches für die Anordnung von Beschränkungsmaßnahmen entsprechend § 10 Artikel 10-Gesetz zuständig war – erfolgt. Dieser Umstand gibt angesichts weiterer Ergebnisse der Beweisaufnahme Anlass für die Feststellung, dass im Arbeitsverhältnis zwischen Fachaufsicht, Anordnungsbehörde und ausführender Behörde die Beachtung wesentlicher formeller Voraussetzungen behördlichen Handelns einschließlich der Grundrechtsbindung als unbeachtlich betrachtet wurde. Dafür spricht auch, dass nach übereinstimmenden Angaben der Zeug_innen die Ergebnisse und Erkenntnisse aus den erfassten und verarbeiteten Kommunikationsdaten überhaupt nichts erbracht haben. Obwohl § 11 Abs. 2

831) *W. K.*, Protokoll-Nr. 35 I, S. 12.

S. 1 Artikel 10-Gesetz die sofortige Beendigung der Überwachungsmaßnahme verlangt, dauerte die Operation nahezu 2 Jahre an. Soweit sich auch ehemalige Vertreter_innen des Bundeskanzleramtes entrüstet darüber geäußert haben, ist dies der Befragungssituation in der öffentlichen Ausschusssitzung geschuldet. Diese eher taktische Positionierung steht dem gegenüber, dass dem BND grundsätzlich der Eindruck vermittelte wurde, dass man mit dem Vorgehen grundsätzlich einverstanden sei.

Auch eine Unterrichtung des Parlamentarischen Kontrollgremiums (PKGr) ist dementsprechend unterlassen worden. Aus § 1 PKGrG ergibt sich, dass die Tätigkeit des Bundesnachrichtendienstes unter dem Gesichtspunkt der parlamentarischen Kontrolle unmittelbar der Bundesregierung zugerechnet wird. Dass die Bundesregierung, insbesondere das Bundeskanzleramt keine Kenntnisse über das Vorgehen des BND bei der Operation GLO[redacted] hatte, vermag sie diesbezüglich nicht zu entlasten. Denn der BND ist dem Bundeskanzleramt unmittelbar zu- und untergeordnet (§ 1 Abs. 1 BNDG). Auch insoweit ist festzustellen, dass auch hier die grundsätzlich erforderliche Unterrichtung der parlamentarischen Gremien als lästige Förmelei und vermutlich eher kontraproduktiv angesehen wurde. Ob zwischen den beteiligten Diensten eine Geheimhaltung vor den aufsichtführenden Stellen und Gremien planmäßig verabredet wurde, ist sehr naheliegend, aber angesichts nicht offengelegter Unterlagen nicht mit letzter Sicherheit feststellbar. Jedoch lassen die auch innerhalb des BND erwogenen Risiken (Strafbarkeit der Beteiligten, Schadensersatzansprüche, öffentliche Empörung bei Bekanntwerden) den Rückschluss zu, dass eine Offenlegung durch den BND planmäßig unterlassen wurde.

Abschließend lässt das Vorgehen des beteiligten amerikanischen Nachrichtendienstes den Rückschluss zu, dass derlei verdeckte Abgriffe unter Inanspruchnahme und Verpflichtung US-amerikanischer Konzernmütter die Rechte der Bürgerinnen und Bürger verletzt, deren Daten von deutschen Konzerntöchtern verarbeitetet werden. Solche Überwachungsmaßnahmen sind strafrechtlich nach den §§ 93 ff., 201 ff. StGB und § 148 TKG zu würdigen. Im Fall der Operation GLO[redacted] richtet sich ein solcher Vorwurf insbesondere gegen die beteiligten und verantwortlichen Beamt_innen des BND.

2. Operation M[redacted]S[redacted]

Nachdem sich der Zeuge *S. L.* in seiner Zeugenvernehmung im Dezember 2014 als benannter Projektleiter für die Operation EIKONAL über eine weitere Operation mit einem amerikanischen Dienst geäußert hatte[832], hatte der Untersuchungsausschuss am 18. Dezember 2014 auf Antrag der Oppositionsfraktionen Unterlagen zu allen vom BND mit Nachrichtendiensten der sogenannten *Five Eyes* durchgeführten Erfassungsprojekten beigezogen.[833] Die Beiziehung und Kenntnisnahme der Materialien und Vorgänge beschränkte sich nach Beurteilung durch den BND und das Bundeskanzleramt dann auf die Operation GL[redacted] sowie eine solche mit einem britischen Nachrichtendienst.

Ob die Nichtübermittlung von weiteren Materialien und Informationen zu anderen Operationen des BND mit Nachrichtendiensten der Five Eyes fehlerfrei erfolgt, lässt sich nicht feststellen.[834] Die Bundesregierung hat nach eigener Auffassung eine Vorlage entsprechender Unterlagen abgelehnt, da diese nach ihrer Auffassung nicht untersuchungsgegenständlich seien. Dass dies der Rechtsprechung des Bundesverfassungsgerichts widerspricht[835] und die Kontrollrechte des Parlamentes einschränkt, hat die Bundesregierung gemeinsam mit den Koalitionsfraktionen an sich abperlen lassen.

Die Umstände der Behandlung der hier bewerteten Operation im Untersuchungsausschuss selbst sind an sich bereits bemerkenswert. Nachdem Unterlagen über die Operation zunächst nur gegenüber den Obleuten und dem Vorsitzenden vorgelegt worden waren, versuchte die Bundesregierung auch durch parallele Unterrichtung des Parlamentarischen Kontrollgremiums (PKGr) gemeinsam mit den Obleuten eine weitere Be-

---

832) *S. L.*, Protokoll-Nr. 26 I, S. 76.

833) Beweisbeschlüsse BND-19 und BND-21.

834) netzpolitik.org vom 5. Juni 2015 „Angezapfte Glasfasern: BND und Kanzleramt verschweigen zehn weitere Operationen zur Internet-Überwachung" (abgerufen am 16.06.2017), https://netzpolitik.org/2015/angezapfte-glasfasern-bnd-und-kanzleramt-verschweigen-zehn-weitere-internet-abschnorchel-aktionen/.

835) BVerfGE 124, 78 (117), http://www.bverfg.de/e/es20090617_2bve000307.html.

handlung in der Beweisaufnahme des Ausschusses möglichst zu vermeiden. Hintergrund waren die kolportierten Drohungen aus Großbritannien.[836] Die Obleute des Ausschusses sollten sich auf diese Weise von der nachdrücklich durch die britische Regierung gewünschten Geheimhaltung der Operation selbst sowie der Einzelheiten überzeugen. Dies war im Ergebnis insofern erfolgreich, als der Ausschuss die schließlich erst im Herbst 2016 für alle Ausschussmitglieder und die berechtigten Mitarbeiter_innen einsehbaren Akten nicht ordnungsgemäß als Beweismaterialien beigezogen hat. Tatsächlich heißt es im entsprechenden Verfahrensbeschluss zur Einordnung beigezogener Materialien, dass Beweismittel immer als MAT A, B oder C bezeichnet werden.[837] Die im Chausseestraßenverfahren zu dieser Operation bereitgestellten Dokumente haben eine solche Bezeichnung nicht erhalten und sind auch in der Geheimschutzstelle des Deutschen Bundestages nicht registriert worden. Genau genommen hat der BND den Parlamentarier_innen Einsichtnahme gewährt. Die Einsichtnahme erfolgte nicht nur aufgrund nach Auffassung des BND und der Bundesregierung zu konsultierender und nicht freigegebener Unterlagen unvollständig. Eine Verwertung für die Ergebnisse des Ausschusses ist nur sehr oberflächlich möglich gewesen.

Parlamentarische Kontrolle hat aus den vorgenannten Gründen auch in diesem Fall zu keinem Zeitpunkt stattgefunden. Entgegen der Auffassung von Bundesregierung, BND und Großer Koalition verdeutlichen die Details der geplanten Operation, dass seitens der Nachrichtendienste die Kooperationsbereitschaft von konkreten Nutzungserwartungen abhängig ist. Tatsächlich sind ausländische Nachrichtendienste nicht berechtigt in Deutschland Kommunikationsdaten zu erheben. Diese Möglichkeit ist allein den deutschen Behörden durch gesetzliche Eingriffsgrundlagen eröffnet (§§ 100a StPO, BKAG, Artikel 10-Gesetz). Wenn ausländische Dienste an den Ergebnissen solcher Erfassungen teilhaben bzw. diese durch eigene Steuerungsmerkmale (Selektoren, Suchbegriffe, Telekommunkationsmerkmale) sogar beeinflussen können und

836) *Süeddeutsche Zeitung* vom 5. Februar 2015, „BND versucht NSA-Aufklärer in die Falle zu locken", http://www.sueddeutsche.de/politik/eklat-im-untersuchungsausschuss-bnd-versucht-nsa-aufklaerer-in-die-falle-zu-locken-1.2337559 (abgerufen am 16.06.2017).

837) Beschluss 4 zum Verfahren: Verteilung von Ausschussdrucksachen, Beweisbeschlüssen und Ausschussmaterialien.

deutsche Behörden als Gegenleistung auch Technik bzw. technische Expertise erhalten, handelt es sich um ein Tauschgeschäft. Die Merkmale dieses Geschäfts haben verschiedene Zeug_innen des BND und auch des Bundeskanzleramtes immer wieder beschrieben. Dass der Austausch von Informationen zwischen den Nachrichtendiensten als notwendiges „Geben und Nehmen" bezeichnet wird, kann letztlich nur die Motive der Beteiligten weichzeichnen. Die Rechtswidrigkeit der Erfassungen bei den Operationen EIKONAL („G 10-Legende" und Steuerung von Selektoren gegen geltendes Recht) und GL[redacted] (unter Legende erschlichener rechtswidriger Zugang zu Kommunikationsverkehrsdaten unter Bruch des Telekommunikationsgeheimnisses) wird hiervon nicht beeinflusst.

Erkennbar geworden ist, dass bis zu den Veröffentlichungen der Dokumente von *Edward J. Snowden* ein derartiges Vorgehen für den BND auch bei einer Kooperation mit einem britischen Nachrichtendienst vorstellbar war. Dass das Projekt gestoppt wurde, war eine unmittelbare Folge der Veröffentlichungen. Allein dies muss als – wenn auch zufälliger – Erfolg des öffentlichen Diskussionsprozesses gewertet werden. Ein Verständnis für die Problemhaftigkeit des beabsichtigten Erfassungsansatzes gemeinsam mit dem britischen Dienst war weder im BND noch in der die Aufsicht führenden Abteilung 6 des Bundeskanzleramtes vorhanden.

Die von britischer Seite offerierten technischen Verlockungen[838] hatten den BND erneut dazu bewegten, trotz fortbestehender Filterproblematik zum Schutz betroffener Bürgerinnen und Bürger einschließlich der Reichweite des zu gewährenden Rechtsschutzes nicht allein für deutsche Staatsangehörige und Firmen eine neuerliche Überwachungsmaßnahme in ernsthafte Erwägung. Ob schon sich nicht abzeichnete, dass die besonderen Bedürfnisse und Ziele der Parteien zufrieden stellend gelöst worden wären, wurde das Projekt – wenn auch in einer sehr frühen Phase – neuerlich offenbar ohne Kenntnis des die Aufsicht führenden Bundeskanzleramtes vorangetrieben. Eine Information erfolgte lediglich lückenhaft und bei hauptsächlicher Betonung des vom

---

838) So u. a. *Spiegel Online* vom 1. Mai 2015 „Operation Monkeyshoulder – BND plante weitere Geheimdienstkooperation am Kanzleramt vorbei", http://www.spiegel.de/spiegel/vorab/geheimdienstkooperation-des-bnd-operation-monkeyshoulder-a-1031643.html, *Stern* vom 2. Juni 2015, „BND-Chef verschwieg lange Operation Monkeyshoulder" http://www.stern.de/investigativ/operation-monkeyshoulder--bnd-chef-verschwieg-umstrittenes-ausspaehprojekt-vor-kanzleramt-6206512.html (abgerufen am 16.6.2017),

BND erwarteten Erfolges. Rechtliche und technische Schwierigkeiten – die bereits zu Tage getreten waren – wurden dabei nicht bekanntgegeben.

Ob und wenn ja welche Gremien von Seiten des BND je in die Durchführung des Projektes auch wegen etwaig einzuholender Genehmigungen eingeweiht worden wären, lässt sich nur spekulieren. Die gegenüber dem Ausschuss zu Tage getretenen Geheimhaltungsbedürfnisse von BND und ehemaligem Partnerdienst[839] lassen eher darauf schließen, dass erneut lediglich eine bruchstückhafte und legendierte Unterrichtung erfolgt wäre.

Ob eine planmäßig durchgeführte Operation mit dem britischen Dienst nicht nur einen rein technischen Mehrwert für den BND sondern auch einen unmittelbaren Mehrwert für die Sicherheit der Bürgerinnen und Bürger gehabt hätte, erscheint zweifelhaft. Nachdem die Bundesregierung mit der Macht der Großen Koalition die Kontrollinstanzen für Kooperationen mit ausländischen Nachrichtendiensten für die Zukunft erheblich eingeschränkt haben, ist zu erwarten, dass künftige Rechtsverstöße durch solche Operationen und deren Maßnahmen noch seltener das Tageslicht sehen werden. Das so tatsächlich ein Mehr an Sicherheit für die Bürgerinnen und Bürger entstehen kann, wird nur der Leichtgläubigste erwarten können.

Wenn tatsächlich, wie in den vorzitierten Medien berichtet, eine weitere Operation zur Erfassung von Massendaten mit einem AND geplant und über lange Zeit vorbereitet wurde, dann belegt dies Ignoranz und Uneinsichtigkeit von Kanzleramt und BND-Spitze. Zur Zeit der heftigen öffentlichen und parlamentarischen Debatten des Sommers 2013 über die Geheimdiensskandale, die sich aus den *Snowden*-Dokumenten ergaben, und während die Verantwortlichen für die Massenüberwachung so taten, als wüssten sie gar nicht, wovon die Rede ist, und leugneten, waren dann gerade diese unterwegs, um genau solche Operationen mit neuem Partner auf den Weg zu bringen und fortzusetzen. Das wäre ein Höhepunkt von Missachtung des immer dringlicher fragenden Parlaments und eine Verhöhnung der Besorgnisse der Öffentlichkeit.

---

839) *Focus* vom 5. Februar 2015, „Briten drohen mit Abbruch aller Kontakte zu Deutschland“ http://www.focus.de/politik/deutschland/geheimdienst-eklat-briten-drohen-mit-abbruch-aller-kontakte-zu-deutschland_id_4454261.html abgerufen am 16.6.2017),.

VII. Nutzung von XKEYSCORE durch BND und BfV

Nach den Veröffentlichungen zu PRISM und TEMPORA wurde mit weiteren *Snowden*-Enthüllungen sowie darauffolgenden Presseberichten im Juli 2013 eine neue Dimension der Internetüberwachung deutlich:[840] Die amerikanische Spähsoftware XKEYSCORE rückte in den Blick der Öffentlichkeit. Hierbei handelt es sich um eines der mächtigsten Werkzeuge der NSA, welches längst auch zum zentralen nachrichtendienstlichen Systemrepertoire der Five Eyes gehört. Auch die deutschen Dienste BND und BfV haben es sich nicht nehmen lassen, XKEYSCORE für eigene Zwecke zu verwenden, erschienen die neuen Möglichkeiten nur allzu verlockend.

Bei XKEYSCORE handelt es sich um ein universelles Programm, das – entwickelt nach den NSA-Zielen „Collect it All", „Process it All", „Sniff it All", „Partner it All", „Exploit it All" und „Know it All"[841] – sowohl zur Gewinnung von Verbindungs- und Metadaten sowie Inhaltsdaten, als auch zur anschließenden automatisierten Analyse verwendet werden kann. Es handelt sich um eine in dieser Ausprägung neuartige Software, die es den Geheimdienstmitarbeiter_innen ermöglicht, in kürzester Zeit Gigabytes von Daten zu erfassen, zu durchsuchen sowie nach frei kombinierbaren Suchkriterien zu filtern. Die Daten können dann direkt in XKEYSCORE für einige Zeit gespeichert und gesammelt werden.[842] Die Software ermöglicht weiterhin eine umfassende und automatisierte Sortierung, Auswertung und Analysierung von Daten.[843] Sowohl Meta-, als

840) *The Guardian* vom 31. Juli 2013, „XKeyscore: NSA tool collects 'nearly everything a user does on the internet'", https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data, abgerufen am 4. Juni 2017.

841) *Glenn Greenwald*, „No Place To Hide", S. 97 (NSA-Folie „New Collection Posture"); *The Washington Post* vom 12. Mai 2014, „'No Place to Hide' by Glenn Greenwald, on the NSA's sweeping efforts to 'Know it All', https://www.washington-post.com/opinions/no-place-to-hide-by-glenn-greenwald-on-the-nsas-sweeping-efforts-to-know-it-all/2014/05/12/dfa45dee-d628-11e3-8a78-8fe50322a72c_story.html, abgerufen am 12.06.2017; vgl. hierzu Kapitel IV.5. – Inhalt und Auswirkungen anlassloser massenhafter Überwachung.

842) Vgl. *The Intercept* vom 1. Juli 2015 „XKeyscore. NSA's Google for the World's Private Communications", abrufbar unter https://theintercept.com/2015/07/01/nsas-google-worlds-private-communications/, abgerufen am 12.06.2017.

843) *Zeit Online* vom 27. August 2015, „Diese Spähsoftware findet jedes Passwort", http://www.zeit.de/digital/datenschutz/2015-08/bfv-verfassungsschutz-was-kann-xkeyscore, abgerufen am 05.06.2017.

auch Inhaltsdaten von „Online-Aktivitäten“ können in Echtzeit überwacht und unter Zuordnung der Teilnehmer_innen[844] i.S.d. § 3 Abs. 4, 5 BDSG verwendbar gemacht werden.

In dem auf Netzpolitik.org veröffentlichten Bericht der BfDI bestätigt diese jene Möglichkeit der Durchsuchung des gesamten Internetverkehrs:

> „Zum Zweck der Nachrichtengewinnung (…) durchsucht XKEYSCORE zu – frei definierbaren und verknüpfbaren – Selektoren (einfachen oder komplexen Fingerprints – Sachstandsbericht, B, VII, 1, a und b) weltweit den gesamten Internetverkehr (IP-Verkehr), d. h. alle im IP-Verkehr enthaltenen Meta- und Inhaltsdaten“.[845]

Damit können selbst nicht öffentliche Nachrichten in E-Mails oder sozialen Netzwerken, Chatbeiträge, Fotos von Webcams, Skype-Gespräche oder live mitgeschnitten werden. Anschließend können laut der BfDI diese

> „getroffenen IP-Verkehre (…) [gespeichert werden] und damit alle in diesen IP-Verkehren auftauchenden Personen (Absender, Empfänger, Forenteilnehmer, Teilnehmer der sozialen Netzwerke etc.).“[846]

Den von *Snowden* enthüllten Dokumenten, ist zu entnehmen, dass das Front-End der Software den Nutzer_innen eine umfassende Darstellungsmöglichkeit der erfassten Informationen bietet. Aufgrund eines Betrachtungstools sei es den Analyst_innen mög-

844) Snowden-Dokument: What is XKEYSCORE?, Powerpoint der NSA vom 25 Februar 2008, MAT A Sek-1b, Bl. 931; *Glenn Greenwald*, „Die globale Überwachung“, S. 221.

845) BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015 unter 1.F.III), veröffentlicht auf netzpolitik.org, https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/, abgerufen am 11.06.2017.

846) BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015 unter 1.F.III), veröffentlicht auf netzpolitik.org, https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/, abgerufen am 11.06.2017.

lich, zum Teil bereits innerhalb des Programms die in annähernder Echtzeit lesbar gemachten Inhalte der Daten direkt ansehen zu können. Dabei werden in der Darstellung auch gleich Informationen miteinander vernetzt angezeigt.[847]

Für den BND

> „ist XKeyscore in Bad Aibling ein wichtiger Baustein bei der Erfassung und Analyse von Internetdaten. Der BND nutzt das Programm ausschließlich für die Aufklärung ausländischer Satellitenkommunikation.“[848]

Belegt ist, dass der BND mittels der Software das Internet nach Informationen und Hinweisen durchsucht und anschließend – auch in XKEYSCORE – umfangreiche Datensammlungen erstellt. Aus den unterschiedlichen Einsätzen aufgrund dieser zahlreichen Funktionen des Programms resultiert auch eine Vielzahl unterschiedlicher Gefahren von Grundrechtsverletzungen.

1. Einsatz von XKEYSCORE im BND

Der BND erhielt XKEYSCORE bereits im Jahr 2007 von der NSA und setzte es in seiner Außenstelle in Bad Aibling ein[849], um massenhaft personenbezogene Meta- und Inhaltsdaten erheben, verwenden und automatisiert analysieren zu können.

Das Programm wurde laut Zeugenaussage des BND-Mitarbeiters *W. K.* zumindest bis 2014 „für die Aufklärung ausländischer Satellitenkommunikation eingesetzt“[850] und damit für die bei diesem Ansatz stattfindende Massenüberwachung des BND in Bad Aibling[851]. Auch für „die Zukunft“ kann der Zeuge einen solchen Einsatz „nicht ausschließen, weil es ein sehr mächtiges System ist.“[852] Auch in zwei weiteren Außenstellen

847) MAT A Sek-1b, S. 930 ff.; vgl. *Spiegel Online* vom 31. Juli 2013, „NSA-System XKeyscore – Die Infrastruktur der totalen Überwachung“.

848) *R. U.*, Protokoll-Nr. 14 I, S. 7.

849) Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der SPD vom 14.08.2013, BT-Drucksache 17/14456, S. 21.

850) *W. K.,* Protokoll-Nr. 22 I, S. 17.

851) Vgl. hierzu Kapitel V.9. Datenübermittlungen des BND an die NSA aus Bad Aibling.

852) *W. K.,* Protokoll-Nr. 22 I, S. 18.

des BND wurde seit Februar 2013 XKEYSCORE getestet.[853] Ob und wie der BND das Programm auch am Kabel einsetzte, konnte im Detail nicht untersucht werden.

Der BND hätte XKEYSCORE aus diversen Gründen nicht verwenden dürfen. Sowohl die Erhebung von Meta- und Inhaltsdaten, als auch die Speicherung, Verarbeitung, Analyse und die Übermittlung von Daten an die NSA widersprachen zum Teil dem geltenden Recht und stellen jeweils separate, eigenständig zu wertende Grundrechtseingriffe dar, die mit den rechtlichen Bedingungen für eine Datenverarbeitung nur schwer in Einklang zu bringen sind (1.a,b). Vor allem aber hätte der BND die Software der NSA nicht blind übernehmen dürfen, sondern hätte technische Vorkehrungen treffen müssen, um eine Funktion und Verwendung dieser im Rahmen des deutschen Rechts zu gewährleisten und somit Grundrechtseingriffen vorzubeugen (1.d). Stattdessen informierte er noch nicht einmal die Fachaufsicht über eine derartige Übernahme amerikanischer Spähsoftware (1.c).

Der BND setzt XKEYSCORE zur „technischen Dekodierung von bestimmten Verfahren“ ein, d. h. um Datenströme lesbar zu machen und „erfassten Verkehr technisch auf[zu]bereiten, damit ihn der Bearbeiter auswerten kann“.[854] Dies geschieht sowohl am laufenden Datenstrom, als „auch mit Daten, die wir woanders haben“.[855] Demnach war die Software für den BND „im Wesentlichen (für uns) ein Analysewerkzeug“.[856] Dies stellt eine qualitativ neue Analysemöglichkeit dar. Die Verwendung des Programms birgt ein enormes Gefahrenpotenzial für Grundrechte, ist daher rechtlich eigenständig zu bewerten und bedarf einer hinreichenden Rechtsgrundlage.

a) Rechtswidriger Einsatz der Spähsoftware durch den BND

Der BND greift mittels XKEYSCORE personenbezogene Meta- und Inhaltsdaten – auch mit Hilfe von NSA-Selektoren – ab, speichert sie, leitet sie weiter an die NSA, rastert sie, wertet sie aus und analysiert sie automatisiert. Hierfür – insbesondere für

853) Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der SPD vom 14. August 2013, Bundestagsdrucksache 17/14456, S. 21.

854) *W. K.*, Protokoll-Nr. 22 I, S. 17.

855) *W. K.*, Protokoll-Nr. 22 I, S. 17.

856) *W. K.*, Protokoll-Nr. 22 I, S. 16.

die eigenständigen Analysemöglichkeit des Programms – fehlte es jedoch an einem Prüfungsschritt, der jeden erneuten Eingriff in die erhobenen Daten gerecht wird. Da das Programm eine Vielzahl neuer Eingriffmöglichkeiten bietet, miteinander kombiniert und gerade die Funktion der automatisierten Analyse eine in Art und Umfang völlig neue Methode im BND darstellt, erscheint eine erneute Prüfung erforderlich, die diesen Besonderheiten gerecht wird.

Aufgrund der technischen Beschaffenheit der Spionagesoftware, die bereits allein zum Zweck massenhafter Überwachung und Durchsuchung sämtlicher IP-Verkehre entwickelt wurde, kann der BND nicht ausschließen, dass zwangsläufig eine enorm hohe Anzahl personenbezogener Daten unbescholtener Personen miterfasst und gespeichert wird.

Die BfDI prüfte mittels einer Stichprobe die Datenbank von XKEYSCORE und musste dabei feststellen, dass das Zahlenverhältnis zwischen Ziel- und Kontaktpersonen 1:15 betrug.[857] Bei einem Trefferdatensatz zu einer Zielperson wurden also Daten zu weiteren 15 Personen erhoben und gespeichert. Dabei handelt sich um Maßnahmen, die nach Auffassung der BfDI für die Aufgabenerfüllung des BND zweifelsfrei nicht erforderlich waren. Denn die sicherlich überwiegende Zahl der sogenannten Kontaktpersonen bieten keinerlei Anlass für nachrichtendienstliche Maßnahmen. Wie auf netzpolitik.org veröffentlicht, habe sich der BND gegebüber der BfDI darauf berufen, dass eine solche Miterfassung unvermeidbar sei.[858] Eine Rechtfertigung kann das jedoch nicht darstellen. Diese Äußerung des BND muss inbesondere vor dem Hintergrund der Möglichkeit von XKEYSCORE, bereits bei Erhebung der Daten eine Zuordnung der jeweiligen Teilnehmer_in zu leisten, gelesen werden. Da der BND diese Meta- und Inhaltsdaten in einer Datenbank speichert, begründet er auch die weitere Gefahr, dass diese zur Grundlage weiterer Verarbeitungsmaßnahmen werden. Das Argument, dass die Erhebung jener Daten als Begleiterscheinung lediglich Mittel zum Zweck seien, kann

857) BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015 unter 1.F.III.1.b), veröffentlicht auf netzpolitik.org, https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/, abgerufen am 11.06.2017.

858) BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015 unter 1.F.III.1.b), veröffentlicht auf netzpolitik.org, https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/, abgerufen am 18.06.2017.

auch nach Ansicht des BVerfG nichts an der grundrechtlichen Relevanz des Eingriffs ändern.[859] Mit Blick auf das Verhältnis zwischen erfassten Ziel- und Kontaktpersonen ist erkennbar, dass es sich hier nicht mehr nur um Einzelfälle handelt, die der BND in seiner Praxis fälschlicherweise überwacht.

Der BND verwandte beim Einsatz von XKEYSCORE auch NSA-Selektoren, d. h. Suchbegriffe, die der ausländische Nachrichtendienst dem BND zur Gewinnung von Informationen zu paketvermittelten Verkehren übermittelte.[860] Dass der Einsatz dieser Selektoren, die er aufgrund von mangelhaften oder fehlenden Deutungen zum Teil nicht lesen und nachvollziehen konnte[861], beim Betrieb von XKEYSCORE, sowie auch die anschließende Ausleitung der hiermit erzielten Treffer an die NSA[862] – jeweils erneute Eingriffe in die betroffenen Grundrechte – im konkreten Einzelfall für die Aufgabenerfüllung des BND erforderlich war, ist ausgeschlossen. Zudem hätte der BND die so unzulässigerweise erlangten Trefferdaten auch nicht weiter verwenden dürfen. Diese Praxis des Nachrichtendienstes stellt eine rechtwidrige Datenverarbeitung dar und widerspricht den Vorgaben aus § 1 Abs. 2 S. 1, § 2 Abs. 1 S. 1 BNDG[863], auf die sich der BND selbst stets bezieht.[864] Der BND hätte die Meta- und Inhaltsdaten größtenteils folglich nicht erheben dürfen und wäre dazu verpflichtet gewesen, sie umgehend zu löschen.

859) BVerfGE 120, 378-433, https://www.bverfg.de/e/rs20080311_1bvr207405.html, Rn. 63 ff.

860) BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015 unter 1.F.I), veröffentlicht auf netzpolitik.org, https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/, abgerufen am 07.06.2017.

861) Vgl. hierzu Kapitel V.7. Verstöße bei der Verwendung von NSA-Selektoren.

862) Vgl. hierzu Kapitel V.8. Datenübermittlungen des BND an die NSA aus Bad Aibling.

863) In den Fassungen vom 30.12.1990 – 10.01.2007 und 11.01.2007 – 30.12.2016.

864) BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015 unter 1.F.IV.1), veröffentlicht auf netzpolitik.org, https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/, abgerufen am 06.06.2017.

b) Umgehung von politischer und fachlicher Kontrolle

Der BND unterließ es, Informationen über den Einsatz von XKEYSCORE an das PKGr zu übermitteln. Dies wäre jedoch zwingend nach § 4 Abs. 1 PKGrG[865] notwendig gewesen. Denn bei dem Einsatz von XKeyscore handelt es sich um einen Vorgang von besonderer Bedeutung über den das PKGr zu informieren gewesen wäre. Es handelte sich um eine neue Analysemöglichkeit und eine undurchsichtige Softwarestruktur aus den Händen eines ausländischen Geheimdienstes.

Der BND hätte die Daten darüber hinaus auch nicht in der Datenbank von XKEYSCORE speichern dürfen. Denn bereits die Speicherung in XKEYSCORE ist rechtswidrig, da der BND hierfür nie eine Dateinanordnung erlangte.[866] Diese wäre jedoch gem § 6 S. 1 BNDG i.V.m. § 14 BVerfSchG[867] eine zwingende Voraussetzung für den Betrieb einer solchen gewesen. Auch hierbei handelt es sich um schwerwiegende Verstöße gegen das BNDG, die zur formellen wie materiellen Rechtswidrigkeit des Verwendens der Datei führte. So erklärte die Datenschutzbeauftragte des BND, Frau *Löwnau,* vor dem Ausschuss:

> „Wir sind intern zu dem Ergebnis gekommen, dass unserer Meinung nach das Fehlen einer Dateianordnung zu einer materiellen Rechtswidrigkeit führt.“[868]

Dass die Dauer der Datenspeicherungen in dieser Datenbank vergleichsweise gering ist, ist der Konzeption des Programms geschuldet, mit dem das Abgreifen und Sammeln gräßmöglicher Datenmengen verfolgt wird, und hat keine rechtlichen Auswirkungen auf das Erfordernis einer Dateianordnung.

Der bei netzpolitik.org veröffentlichte Bericht der BfDI zur rechtlichen Bewertung lässt implizit die Behauptung des BND erkennen, es handele sich vorliegend nicht um eine

865) In der Fassung vom 29. Juli 2009 (davor § 2).

866) *Löwnau*, Protokoll-Nr. 72 I, S. 43, 62; BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015 unter 1.F.II), veröffentlicht auf netzpolitik.org, https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/, abgerufen am 07.06.2017.

867) In den Fassungen vom 01.01.2000 – 10.01.2007, 11.01.2007 – 04.08.2009 sowie vom 05.08.2009 – 20.11.2015.

868) *Löwnau*, Protokoll-Nr. 72 I, S. 88.

automatisierte Datei i.S.d. § 11 BNDG[869] i.V.m. § 46 Abs. 1 Nr. 1 BDSG.[870] Dies wäre nicht nur falsch, sondern würde zudem eine irritierende Ausrede darstellen. Ein Verständnis innerhalb der Behörde von der verwendeten Technik und das Wissen über die Bedeutung ihrer Verwendungen sind von enormer Wichtigkeit für eine rechtmäßige und grundrechtskonforme Tätigkeit des BND. Es ist dem BND vorzuwerfen, dass er nicht wie rechtlich vorgesehen eine Dateianordnung erstellte und folglich ungerechtfertigt in Grundrechte eingriff.

Dass er dabei in XKEYSCORE auch Daten von für ihn unwichtigen Personen absichtlich (mit)speicherte, ist besonders erschreckend. Anders als vom BND behauptet, ist hierfür unerheblich, dass diese gespeicherten Daten angeblich „ausgeschnitten“ und nicht weiter verwendet wurden. Der Grundrechtseingriff war bereits ungerechtfertigt vollzogen.[871]

c) Ungenügende IT-Sicherheitsprüfung

Den *Snowden*-Dokumenten ist zu entnehmen, welch enormes Spähpotential in der Software der NSA steckt. Es handelt sich um ein vielseitiges Erfassungs- und Verarbeitungsprogramm, welches zur umfassenden Aufklärung in Echtzeit – vor allem auch aufgrund der metadatenzentrierten Analysemöglichkeit – dienen kann. Eine Besonderheit besteht in der umfassenden Verbreitung des Programms über die ganze Welt. Bereits im Jahr 2008 waren mehr als 700 Server an über 150 Standorten global verteilt[872], wo die Daten erhoben, direkt gespeichert und verarbeitet werden, bevor sie weiterfließen. Vor allem die NSA verfolgt hiermit das Ziel umfassender Informationsgewinnung.[873] Eine einzige Suchanfrage reiche aus, um eine Vielzahl von Standorten

869) In der Fassung vom 23.05.2001 bis 30.12.2016.

870) BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015 unter 1.F.II), veröffentlicht auf netzpolitik.org, https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/, abgerufen am 07.06.2017.

871) BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015 unter 1.F.IV.2), veröffentlicht auf netzpolitik.org, https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/, abgerufen am 07.06.2017; Für Näheres zur fehlenden Dateianordnung siehe Kapitel V.10. Behinderungen der Arbeit der Bundesbeauftragten für den Datenschutz.

872) MAT A Sek-1b, Bl. 935.

873) Vgl. *taz* vom 2. August 2013, „Wie groß ist der große Bruder schon?“.

zeitgleich abfragen und miteinander vernetzt darstellen zu können.[874] Ob hier bereits die Standorte des BND inbegriffen sind, bleibt fraglich. Der BND-Zeuge *W. K.* beteuerte vor dem Ausschuss:

> „Ich (…) habe ja auch die Presse der letzten Monate gelesen, dass es angeblich da ein Netzwerk geben soll mit Erfassungssystemen, XKEYSCORE. So ist es bei uns nicht. Wir haben das als Stand-alone-System für die Analyse. Wir sind an keinem Netzwerk beteiligt mit den USA, und unsere Erfassungssysteme sind die Antennen und technischen Geräte, die wir an den Außenstellen haben."[875]

Der BND hat dies zwar beteuert, konnte es aber nicht fundiert belegen, denn einen umfassenden Einblick in die Software hinter XKEYSCORE hatte er ebensowenig, wie es eine hinreichende Bewertung auf der Basis einer IT-Sicherheitsprüfung gab. Eine solche Prüfung hätte vor Ort durch das BSI vorgenommen werden müssen und zwar für das laufende Programm. Doch dies geschah vorliegend nicht.[876]

Der BND selbst führte in Bad Aibling Überprüfungen allgemein nur unzulänglich durch. Nach Zeugenaussagen gab es in der JSA zwar Tests, diese richteten sich jedoch nach der Frage, ob die Systeme die jeweiligen Aufgaben erfüllen. So sagte der BND-Mitarbeiter *T. B.* allgemein ausführend vor dem Ausschuss:

> „Es war sehr schnell klar, dass wir nicht jedes Programm bis in die Details kontrollieren können" (…) „Wir haben [daher] nicht für jedes neu eingesetzte Modul oder verbesserte Modul einen umfangreichen Test über ein halbes Jahr gefahren. Das wäre nicht möglich gewesen und auch nicht zielführend. (…) Es gab Tests dieser Module, ob sie genau ihre Aufgaben erfüllen".[877]

874) MAT A Sek-1b, S. 930 ff., v. a. 952; vgl. *Spiegel Online* vom 31. Juli 2013, „NSA-System XKeyscore – Die Infrastruktur der totalen Überwachung".

875) *W. K.*, Protokoll-Nr. 22 I, S. 16.

876) Vgl. hierzu Kapitel V.5. – Unzulängliche BSI-Prüfung.

877) *T. B.*, Protokoll-Nr. 20 I, S. 37.

Hierzu muss gesagt werden, dass die Überprüfung von XKEYSCORE schon deshalb nicht vollumfänglich möglich war, weil der BND den Quellcode der Software von der NSA nie erhielt.[878] Er begnügte sich mit den Zusicherungen und Angaben der NSA. Durch Medienberichte wurde 2014 bekannt, was vielleicht selbst der BND schon lange vermutete.[879] Den Berichten zufolge beinhaltet der Quellcode Details über Fähigkeiten des Programms, die der BND nicht ohne weiteres einsetzen dürfte. Eine fehlende Einsicht kann demnach verheerende Auswirkungen haben (vgl. Kapitel 4 Massenüberwachung).

Die NSA sicherte zu, dass das System technisch stets auf dem neusten Stand sei und auch bei den deutschen Geheimdiensten immer wieder durch NSA-Mitarbeiter_innen mit neuesten Updates versehen wurde. Hier hätte der BND dafür sorgen können und müssen, die Grundrechtseingriffe zu minimieren: Indem er selbst Wartung und Updates übernommen hätte. Voraussetzung wäre gewesen, dass der BND die Software und die neuesten Updates auch technisch verstanden und unter seiner Kontrolle hatte.

XKEYSCORE gilt als Software, die sich durch zahlreiche Module für bestimmte Plugins erweitern lässt.[880] Es ist nicht bekannt, welche Version von XKEYSCORE der BND verwendete, oder was die NSA bei ihren eigenständigen Updates ohne Kontrolle durch eine/n BND-Mitarbeiter_in tatsächlich installierte.

Teilweise haben BND-Mitarbeiter_innen die NSA-Programme als „Blackbox“ verstanden, da sie nach eigenen Angaben diese nicht in vollem Umfang überblickten.

So sagte der Zeuge T. B. zum allgemeinen Verständnis über die Hard- und Software der NSA vor dem Untersuchungsauschuss aus:

> „Wir wollten durchaus an der einen oder anderen Stelle wissen, wie es funktioniert, und dann ist aber sehr schnell auch herausgekommen, dass es selbst die Mitarbeiter des anderen Partners nicht wussten. Im

---

878) *T. B.*, Protokoll-Nr. 20 I, S. 37.

879) Vgl. NDR vom 03. Juli 2014 „Quellcode entschlüsselt: Beweis für NSA-Spionage in Deutschland“, http://www.ndr.de/nachrichten/investigation/Quellcode-entschluesselt-Beweis-fuer-NSA-Spionage-in-Deutschland,nsa224.html, abgerufen am 12. Juni 2017.

880) Vgl. *Spiegel Online* vom 31. Juli 2013, „NSA-System XKeyscore – Die Infrastruktur der totalen Überwachung“.

> Grundsatz muss jemand, der ein Formel 1 Auto fährt, es nicht konstruieren können.“[881]

Die Schlussfolgerung des BND:

> „Wenn wir die Systeme einzeln nicht verstehen, dann müssen wir ganz knallhart alles das, was diese Blackbox verlässt, uns anschauen und genauestens filtern. – Und das war dann der Punkt, an dem wir einfach unseren Schwerpunkt gesetzt haben.“[882]

Die Schlussfolgerung der Oppositionsfraktionen:

Der BND hätte die Software von Dritten prüfen und zertifizieren müssen, um zu gewährleisten, dass das Programm den Anforderungen entspricht. Ohne eine fundierte Kenntnis über die Funktionstüchtigkeit und Arbeitsweise darf ein solches Werkzeug nicht eingesetzt werden.

Der BND hätte gerade bei XKEYSCORE äußerst hohe Anforderungen an sein Verständnis über die verwendete Software stellen müssen, da er das Ziel und die Intentionen der NSA kannte und XKEYSCORE den Geheimdiensten Zugriff auf weite Teile der Internetkommunikation erlaubt. Ein auch nur irgendwie gearteter Zugriff der NSA auf das im BND eingesetzte Programm muss ausgeschlossen sein. Vor allem, da Medienberichten zufolge das Programm die Erfassung in Echtzeit ermöglicht und einen „durchlaufenden Pufferspeicher“ umfasst, der „ALLE ungefilterten Daten“ beinhaltet.[883] Ein Zugriff der NSA auf solche ungefilterten Daten wäre rechtswidrig. Werden die erfassten Daten auf Basis ihrer Metadaten indexiert und miteinander verknüpft, so lassen sich Informationen generieren, die in ihrem Ausmaß und ihrer Qualität eine anlasslose und massenhafte Überwachung ermöglichen.

881) *T. B.*, Protokoll-Nr. 20 I, S. 21.

882) *T. B.,* Protokoll-Nr. 20 I, S. 21.

883) MAT A Sek-1b, vgl. *Spiegel Online vom 31. Juli 2013*, „NSA-System XKeyscore – Die Infrastruktur der totalen Überwachung“.

2. Einsatz von XKEYSCORE im BfV

Untersuchungen des Ausschusses haben ergeben: Ab Juni 2013 wurde die Spähsoftware XKEYSCORE im BfV installiert.[884] Auf einem Rechner in Berlin[885] wurde sie ab September 2013 über Jahre hinweg „getestet". So musste der Zeuge *A.Sch*. im Dezember 2015 vor dem Untersuchungsausschuss noch erklären:

> „Der Wirkbetrieb hat meiner Meinung nach bis heute nicht begonnen."[886]

Im Sommer 2016 wurde XKEYSCORE dann offiziell für die Analyse gespeicherter Daten eingesetzt und soll bis heute dort standardmäßige Verwendung finden. Über den tatsächlichen Einsatz ist nur wenig bekannt, weil, so das BfV, der Untersuchungszeitraum endet bevor die Software tatsächlich im sogenannten Wirkbetrieb eingesetzt wurde. Die Phase während des Untersuchungszeitraums stelle lediglich einen Probezeitraum dar. Die Darstellung, dass es sich bei der vorliegenden Verwendung um einen sogenannten Probebetrieb handelt, ist nach der Auffassung der Opposition im Ausschuss unzutreffend. Sie täuscht über die Arbeit unter Verwendung von echten Daten hinweg.

Das BfV beteuerte stets, es setze das Programm nicht zur Datengewinnung, sondern lediglich zur automatisierten Analyse des bereits vorhandenen Datenbestands sei.[887] Das BfV verwendete die Version von XKEYSCORE des BND. Eine technische Modifikation dieser fand nicht statt, so der Zeuge *A.Sch.*[888]

Diese im BfV bereits vorhandenen Daten seien im Rahmen von G 10-Maßnahmen bereits sowieso erhobene Daten.[889] Die Bedeutung des neuen Programms für das BfV beschrieb der Zeuge Treuenfels vor dem Ausschuss wie folgt:

---

884) *A. Sch.*, Protokoll 77 II – Auszug offen, S. 13.

885) *Delmdahl*, Protokoll-Nr. 86 I, S. 20.

886) *A. Sch.*, Protokoll 77 II – Auszug offen, S. 19.

887) *A. Sch.*, Protokoll 77 II – Auszug offen, S. 26.

888) *A. Sch.*, Protokoll 77 II – Auszug offen, S. 19.

889) Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der SPD vom 14.08.2013, BT-Drucksache 17/14456, S. 22.

> „Und durch XKeyscore, wenn es dann mal in den Wirkbetrieb geht, wäre man in der Lage, erst mal eine viel größere Anzahl an Protokollen darzustellen; man wäre aber auch in der Lage, mit einem analytisch anderen Ansatz an die Daten, an die Analyse heranzugehen. Unsere bisherige TKÜ-Anlage kommt noch sehr aus einer Telefonwelt, arbeitet sequenziell Daten ab, hört: Was ist da telefoniert worden? – Mit XKeyscore kann man da vertiefte Analysen machen.“[890]

Aber gerade in dieser Kombination – bereits erhobene Daten werden mittels XKEYSCORE erneut analysiert – liegt eine Datenverarbeitung, die für die Tätigkeit des BfV von neuer Qualität ist und ein erhebliches Potenzial mit sich bringt. Die hierin liegende Möglichkeit den gesamten Datenpool sämtlicher G 10-Anordnungen automatisiert zu verknüpfen und zu analysieren, stellt eine völlig neue Form mit erhbelicher Intensität der Datenverarbeitung dar und eröffnet zudem auch die Chance der Erhebung neuer Daten. Für diese eigenständige Analysemöglichkeit bedarf es einer eigenständigen und hinreichend konkreten Rechtsgrundlage. Eine solche ist vorliegend jedoch nicht ersichtlich.

Der Datenbestand des BfV generiert sich ursprünglich aus Inhaltsdaten verdächtiger Zielpersonen, die – da es sich stets um Grundrechtseingriffe handelt – das BfV nach § 3 Artikel 10-Gesetz nur auf Grundlage von speziellen und einzelfallbezogenen G 10-Beschränkungsmaßnahmen in Deutschland überwachen darf.

Bei solchen Abgriffen fallen stets auch zahlreiche Metadaten an, die das BfV bislang in ihrer Masse nicht auswerten konnte. Dass er das überhaupt dürfte, erscheint zweifelhaft. Die Metadaten enthalten aufgrund ihrer besonderen Qualität äußerst relevante Informationen und lassen über die Inhaltsdaten hinaus aufschlussreiche Rückschlüsse auf Verhaltensweisen zu und ermöglichen die Darstellung von Beziehungsgeflechten, vordringend bis in die letzte Tiefe sämtlicher Beziehungsebenen. Die automatisierte Analyse von Metadaten war für das BfV somit eine wesentliche Komponente der Spähsoftware, konnte es zuvor doch hauptsächlich Inhaltsdaten aus E-Mails oder Telefonaten erfassen. Die BfV-eigene Anlage zur Erfassung und Auswertung von Daten

---

890) *Treuenfels*, Protokoll-Nr. 94 I, S. 11.

PERSEUS, die weiter zur Datenerfassung eingesetzt wurde, wertete die dazugehörigen Metadaten kaum aus.[891] XKEYSCORE hingegen erkennt in den Daten u.a. Anwendungen und Protokolle. Es kann die über sie transportierte Kommunikation dekodieren, d. h. lesbar machen[892] und bietet so viel weitergehende Möglichkeiten der Überwachung. Mit XKeysore ist es möglich, einzelne Personen oder Geräte über verschiedene Formen der digitalen Kommunikation zu verfolgen und umfangreiche Profile der Nutzer_innen anzulegen.[893] XKEYSCORE soll vor allem die Suche nach bislang unbekannten Verdächtigen und deren weitere Überwachung erleichtern. Die Dekodierung soll es ermöglichen, Personen ausfindig zu machen, die sich im Internet anonym verhalten. Datenströme werden demnach nach „abweichenden Ereignissen“ durchforstet. Dabei kann praktisch fast jede Person potentiell verdächtig werden.

Mit XKEYSCORE war es dem BfV nun auch möglich, ganze Fingerprints von überwachten Personen zu erstellen.[894]

Laut Medienberichten schuf das BfV im Zeitraum der Übernahme von XKEYSCORE in den Wirkbetrieb rund 75 neue Arbeitsplätze, um die Gewinnung, Verarbeitung und systematische Auswertung von massenhaft Daten aus dem Internet zu bewältigen.[895] Bereits im April des Jahres 2012 trafen sich BfV- und BND-Mitarbeiter_innen in Bad Aibling um sich von Mitarbeiter_innen der NSA in metadatenzentrierter Verhaltensanalyse schulen zu lassen.[896]

---

891) *Zeit Online* vom 27. August 2015, „Diese Spähsoftware findet jedes Passwort“, http://www.zeit.de/digital/datenschutz/2015-08/bfv-verfassungsschutz-was-kann-xkeyscore, abgerufen am 05.06.2017.

892) *Delmdahl*, Protokoll-Nr. 86 I, S. 41; A.Sch., Protokoll-Nr. 77 II – Auszug offen, S. 11.

893) *Zeit Online* vom 26. August 2015, „Suche NSA-Spionagesoftware, biete deutsche Daten“, http://www.zeit.de/digital/datenschutz/2015-08/xkeyscore-nsa-verfassungsschutz, abgerufen am 04.06.2017.

894) *Delmdahl*, Protokoll-Nr. 86 I, S. 71.

895) *netzpolititk.org* vom 15. April 2015, „Geheime Referatsgruppe: Wir enthüllen die neue Verfassungsschutz-Einheit zum Ausbau der Internet-Überwachung (Updates)“, https://netzpolitik.org/2015/geheime-referatsgruppe-wir-praesentieren-die-neue-verfassungsschutz-einheit-zum-ausbau-der-internet-ueberwachung/, abgerufen am 07.06.2017.

896) Snowden-Dokument: NSA’s Counterterrorism (CT) Relationship with the BND and the BfV, Information Paper der NSA vom 8. April 2013, https://edwardsnowden.com/2014/06/18/nsas-counterterrorism-ct-relationship-with-the-german-foreign-intelligence-service-bnd-and-the-german-federal-office-for-the-protection-of-the-constitution-bfv/, abgerufen am 12.06.2017.

a) Verknüpfungsmöglichkeiten

Die Verknüpfung der Daten aus G 10-Aufkommen mit einer automatisierten metadatenzentrierten Analyse stellt auch aufgrund der Geschwindigkeit und der Masse der auswertbaren Daten eine völlig neue Form der Verarbeitung bzw. Auswertung dar. Die damit erstellbaren Informationen reichen in ihrem Aussagegehalt weit über die in der bisherigen Praxis des BfV ermittelten Daten hinaus und sind daher als eigenständige Grundrechtseingriffe zu werten, die in ihrer Form eine besondere Intensität aufweisen.

Das BfV wurde bei der Anwendung von XKEYSCORE anfangs vom BND unterstützt, der ja schon jahrelange Erfahrung damit hatte. Ein BND-Mitarbeiter wurde deswegen eigens zum BfV abgeordnet.[897] Seine Aufgabe war die Installation von Software und Updates sowie die Schulung der BfV-Mitarbeiter_innen.

Etwas war für den BND besonders interessant, der Zugang zu bestimmten Daten, zu deren Erfassung nur der inländische Geheimdienst, das BfV, befugt ist. Ein Tauschgeschäft erschien ihm daher gelegen, wusste er doch, dass die NSA im Besitz der unter Geheimdiensten weltweit begehrten Spähsoftware war und sich auch stets darum bemühte diese an verschiedensten Orten sinnig zu plazieren. Es wurde daher vor allem im BND verstärkt angestrengt, dem BfV dieses Programm zur Datengewinnung und -analyse anzubieten.[898] Einmal zur Verfügung gestellt, sollte es die Basis der zur Verfügung stehenden Daten ausweiten. Hierin liegt der Clou: Der BND vermittelte daher zwischen den Diensten. Als positive „Begleiterscheinung“ sollte auf diese Weise auch er, der BND, in den Besitz der begehrten Daten des BfV geraten.[899]

Der BND interessierte sich vonehmlich für jene Informationen, die neben den Hauptinformationen aufgrund von G 10-Anordnungen dem BfV zur Verfügung standen. Mit Hilfe von XKeyscore ließen sich diese, wie beispielsweise Daten über Kommunikationspartner_innen, in besonderem Umfang gewinnen und analysieren.

897) *A. Sch.*, Protokoll-Nr. 77 II – Auszug offen, S. 16 f.

898) Über das Angebot von BND und NSA: *Treuenfels*, Protokoll-Nr. 94 I, S. 7, 13.

899) Datenübermittlung aufgrund der Zuständigkeiten nur über SIGINT-Behörden möglich: *Treuenfels*, Protokoll-Nr. 94 I, S.31.

Bereits im Frühjahr 2011 gelang es dem BND über seine Abteilung 6 für sein Vorhaben, den ersten Kontakt zwischen BfV und NSA herzustellen.[900] In der Folge schlossen die drei Nachrichtendienste einen Vertrag mit dem Titel „Terms of Reference" (ToR) ab.[901]

Der Zeuge Treuenfels erklärte vor dem Ausschuss:

> „ich weiß, dass der Bundesnachrichtendienst beispielsweise Daten an das Bundesamt für Verfassungsschutz [jeweils über die Fachabteilungen] übermittelt. Das sind sicherlich auch Daten aus SIGINT-Aufkommen."[902]

Ob es sich hierbei um Routineverkehre aus dem Ausland handelt, die automatisiert übermittelt wurden, konnte der Zeuge nicht sagen.[903] Das BfV verwendete XKEYSCORE auch, um neue Filterkriterien und –begriffe zu entwickeln.[904] Laut der BfDI *Andrea Voßhoff* wurden auch dem BND Suchbegriffe von inländischen Behörden übermittelt.[905]

Zur Art und Weise der Datenübermittlung, bzw. zur Frage, ob es eine feste Leitung zwischen BND und BfV gibt, einen sogenannten Austauschserver, über den die Daten übermittelt werden, antwortete der Zeuge Treuenfels:

> „Kann ich nichts zu sagen; weiß ich nichts zu. Also, es gibt ein E-Mail-Verfahren. Und wenn wir ein Schreiben an den BND schicken, dann schicken wir da eine E-Mail."[906]

900) *Treuenfels*, Protokoll-Nr. 94 I, S. 7, 12.

901) Vgl. auch *Zeit Online*, „XKeyscore – das Dokument", Veröffentlichung vom 26.08.2015, http://www.zeit.de/digital/datenschutz/2015-08/xks-xkeyscore-vertrag, abgerufen am 04.05.2017.

902) *Treuenfels*, Protokoll-Nr. 94 I, S. 15.

903) *Treuenfels*, Protokoll-Nr. 94 I, S. 15.

904) *Delmdahl*, Protokoll-Nr. 86 I, S. 18.

905) BfDI: Rechtliche Bewertung zum Sachstandsbericht vom 30. Juli 2015 unter 1.E.I), veröffentlicht auf netzpolitik.org, https://netzpolitik.org/2016/geheimer-pruefbericht-der-bnd-bricht-dutzendfach-gesetz-und-verfassung-allein-in-bad-aibling/, abgerufen am 07.06.2017.

906) *Treuenfels*, Protokoll-Nr. 94 I, S. 15.

Warum das BfV die Daten nicht direkt an die NSA, sondern über den BND übermittelte, konnte er nicht erklären.

> „SIGINT-Behörden unterliegen offensichtlich noch mal anderen Kautelen als Inlandsnachrichtendienste. Es gibt auch noch mal spezielle Anforderungen. Fernmeldeermächtigungen beispielsweise braucht man, wenn man im Bereich SIGINT arbeitet, was im Bereich BfV nicht erforderlich ist. Also, es gelten einfach noch mal andere Spielregeln. Und die Praxis war, dass der Kontakt zwischen BfV und NSA über BND lief.“[907]

b) Der Deal: Software gegen Daten

In BfV-internen Akten heißt es:

> „Die Tatsache, dass BND und NSA mit insgesamt sieben Vertretern angereist waren, deutet darauf hin, dass dort ein sehr hoher, interner Druck (von höherer Ebene) existiert. Die Ausführungen beider Behörden ließen mehrfach darauf schließen, dass der produktive Einsatz von xkeyscore im BfV ab (…) Oktober 2012 kein willkürlich definiertes und kein unverbindliches Ziel darstellt.“[908]

Das BfV erhielt die Spionagesoftware von der NSA folglich nicht ohne Gegenleistung. Der zugrundeliegende Vertrag zwischen den drei Parteien ist geheim eingestuft,

Veröffentlichungen von *Zeit Online* berufen sich jedoch auf Details des Abkommens, die deutlich erkennen lassen, dass ein Tauschgeschäft vereinbart wurde. Das BfV verpflichtete sich demnach, so viele Daten aus Maßnahmen wie möglich der NSA zu überlassen[909], soweit er sie auf der Grundlage von G 10-Anordnungen mittels

907) *Treuenfels*, Protokoll-Nr. 94 I, S. 31.

908) *Treuenfels*, Protokoll-Nr. 94 I, S. 32., Aktenvorhalt: Vermerk vom 13. Juli 2012, „Rohdatenanalyse”, MAT A BfV-9/1 (Tagebuchnummer 21/14 – GEHEIM), Anl. 01, Band 1, Bl. 82 (VS-NfD).

909) *Flisek* (SPD) über den in *Zeit Online* veröffentlichten Vertrag, in: Genkova, Protokoll-Nr. 89 I, S. 108.

XKEYSCORE extrahieren konnte. *Zeit Online* zitierte die Passage des Vertrages wie folgt:

> „The BfV will: To the maximum extent possible share all data relevant to NSA's mission."[910]

Der BfV-Mitarbeiter André Treuenfels erklärte:

> „Also, allgemein kann ich sagen, dass es Übermittlungen [an amerikanische Dienste] gegeben hat."[911]

Das Ziel, das in dem hier zitierten Vertragsabschnitt deutlich wird, ist die größtmögliche Datenübermittlung ohne klare Grenzen. Ein Abkommen, dass es zumindest schwer macht, anzunehmen, dass diese Kooperation nicht auch zu Lasten von Grundrechtsträger_innen geht. Verstärkt wird diese Vermutung durch das bewusste Umgehen der Kontrollen durch die Rechtsaufsicht.

c) Spähprogramm – nur mal getestet?

Über einzelne Datenübermittlungen ist bislang wenig bekannt, da sich das BfV für den Untersuchungszeitraum stets darauf berief, lediglich getestet zu haben. Doch als sich der Ausschuss mit dieser Probephase näher beschäftigte, musste er feststellen, dass diese Begrifflichkeit wohl mehr verschleierte, als sie klar definierte.

Einige Ungereimtheiten traten zum Vorschein. Sie sind eng mit der bereits zu Beginn herrschenden Skepsis im BfV über den Einsatz von XKEYSCORE verwoben. Weshalb nach Ansicht von BND- und NSA-Mitareiter_innen schon am Anfang „die Schaffung der Möglichkeit der Zusammenarbeit der drei Dienste schwierig war".[912]

---

910) *Zeit Online* vom 26. August 2015, „XKeyscore – das Dokument", http://www.zeit.de/digital/datenschutz/2015-08/xks-xkeyscore-vertrag, abgerufen am 4. Mai 2017.

911) *Treuenfels*, Protokoll-Nr. 94 I, S. 34.

912) *Treuenfels*, Protokoll-Nr. 94 I, S. 32, Aktenvorhalt: Vermerk vom 13. Juli 2012, „Rohdatenanalyse", MAT A BfV-9/1 (Tagebuchnummer 21/14 – GEHEIM), Anl. 01, Band 1, Bl. 80 (VS-NfD).

aa) Ungereimtheit Nr. 1: Verwendung von Echtdaten

Am 5.und 6. Oktober 2011 führten die NSA-Mitarbeiter_innen in Bad Aibling dem BfV das Programm vor. Bereits bei dieser ersten Vorführung sollen Echtdaten verwendet worden sein, die das BfV hierfür bereitstellte.[913] Die Zeugin *Genkova* berichtete, dass Echtdaten ab dem 30. September 2013 bis zum Ende des Proof of Concepts verwendet wurden.[914]

Es folgten mehrere Schulungen die gemeinschaftlich mit BfV-, BND- und NSA-Mitrabeiter_innen abgehalten wurden, sowie eine lang andauernden „Testphase“.

„Testphase“ bedeutet dabei vor allem eines: dass nicht die Daten aus allen G 10-Maßnahmen des BfV verwendet wurden, sondern nur von einigen. In jedem Fall wurden auch vor Erstellung des für den Echtbetrieb nötigen ‚Sicherheitskonzepts‘ hierfür echte personenbezogene Daten aus sogenannten G 10-Aufkommen verwendet. Diese griff das BfV zuvor mittels der PERSEUS-Anlage ab.[915] Diese Verwendung stellt bereits eine Datenverarbeitung i.S.d. BDSG dar. Die Übermittlung ist im Sinne des BDSG auch eine Form von Datenverarbeitung. Dieser Ansicht war auch der BfDI *Peter Schaar*.[916] Gem. § 3 Abs. 4 S. 2 Nr. 3 b BDSG handelt es sich auch um Übermittlungen, wenn gegenüber einem Dritten – hier die NSA und der BND – gespeicherte oder durch Datenverarbeitung gewonnene personenbezogene Daten in der Weise bekannt gegeben werden, dass „der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft“. Damit reicht es aus, wenn NSA und BND nur die Möglichkeit zu Kenntnisnahme erlangen und die entscheidende Aktivität anschließend von ihnen ausgeht.[917] Das BfV hat eine solche Möglichkeit zweifelsfrei geschaffen, indem die Mitarbeiter_innen der drei Nachrichtendienste sich gegenseitig unter der Verwendung echter personenbezogener Daten schulten.

---

913) *Zeit Online* vom 26. August 2015, „Suche NSA-Spionagesoftware, biete deutsche Daten“, http://www.zeit.de/digital/datenschutz/2015-08/xkeyscore-nsa-verfassungsschutz, abgerufen am 04.06.2017.

914) *Genkova*, Protokoll-Nr. 89 I, S. 109.

915) *Genkova*, Protokoll-Nr. 89 I, S. 104.

916) *Zeit Online* vom 26. August 2015, „Suche NSA-Spionagesoftware, biete deutsche Daten“, http://www.zeit.de/digital/datenschutz/2015-08/xkeyscore-nsa-verfassungsschutz, abgerufen am 04.06.2017.

917) Vgl. *Erbs/Kohlhaas/Ambs*, BDSG, § 3 Rn. 23 f.; *Roßnagel*, DatenschutzR-HdB/Schild, Kap. 4.2 Rn. 72.

Interne Akten belegen, dass die NSA bewusst darauf abzielte, mit echten Daten gemeinsam zu üben. So heiß es, die

> „NSA erwartet einen schnellen Einsatz mit Echtdaten und zeitnah, erste Arbeitsergebnisse („want working results"). BND weist darauf hin, dass die Zeit für Testen und Ausprobieren („playdata") bereits im Oktober in Bad Aibling abgeschlossen wurde. Darüber hinaus sei kein ernsthaftes Beschäftigen mit dem System zu erreichen, solange nur mit Testdaten erprobt würde („playdata vs. Hunting instinct").[918]

Dass das BfV grundsätzlich auch willens war, „so viele Daten wie möglich" zu übermitteln ist aus dem von ihm unterzeichneten Vertrag zu lesen. Doch vorliegend ist keinerlei Erforderlichkeit für die Übermittlung dieser Daten an BND und NSA gegeben.

Das BfV war sich der Brisanz dieser in der Testphase verwendeten Echtdaten bewusst. Schon im Juli 2012 warnte eine Abteilung des BfV davor, dass bereits die Probephase der Software aufgrund der Verwendung echter Daten „weitreichende rechtliche Folgen" haben könnte. So müssten Mitarbeiter_innen hinzugezogen werden, um die Art und den Umfang des Programms testen und einschätzen zu können, die nicht dazu befugt seien, die hier verwendeten personenbezogenen Daten einzusehen. Zu den näheren Umständen gab das BfV jedoch keine Auskunft."[919] Wenn es die Problematik doch schon hinsichtlich der Kenntnisnahme durch eigene Mitarbeiter_innen feststellte, fragt sich, weshalb es dies bei Mitarbeiter_innen von NSA und BND nicht so eng nahm.

Eine Erforderlichkeit für die Verwendung echter Daten für Testzwecke ist ebensowenig erkennbar, wie jene für eine Übermittlung in diesem Rahmen an BND und NSA.

Der Zeuge *André Treuenfels* beteuerte vor dem Auschuss, es sei

---

918) *Treuenfels*, Protokoll-Nr. 94 I, S. 31 f., Aktenvorhalt: Vermerk vom 13. Juli 2012, „Rohdatenanalyse", MAT A BfV-9/1 (Tagebuchnummer 21/14 – GEHEIM), Anl. 01, Band 1, Bl. 80 (VS-NfD).

919) Zeit Online vom 26. August 2015, „Suche NSA-Spionagesoftware, biete deutsche Daten", http://www.zeit.de/digital/datenschutz/2015-08/xkeyscore-nsa-verfassungsschutz, abgerufen am 4. Juni 2017.

> „einfach dieser Notwendigkeit geschuldet, mit echten Daten zu testen, weil die Kommunikationswelt einfach so komplex ist, dass Sie diese Daten nicht mit selbst generierten Fake-Daten, Spieldaten ausreichend nachstellen können. (…) [Und] weil man ja gar nicht weiß, was von Verdächtigen im Rahmen von G 10-Maßnahmen eingesetzt wird. Deswegen kann man das nicht vorher nachbauen oder antizipieren.“[920]

Die Zeugin *Monika Genkova* sagte hinsichtlich der Verwendung von Echtdaten aus:

„Die Fachabteilung hat begründet, dass es mit Testdaten nicht hinreichend aussagekräftig wäre. (…) Aufgrund der Vielzahl der Protokolle, die analysiert werden sollen. Und es wurde begründet, dass man diese Protokolle anhand von Testdaten nicht hinreichend nachstellen könnte, um zu aussagekräftigen Ergebnissen zu kommen.“[921] Der Verweis die Komplexität des Internets kann hier aber nicht genügen. Es erscheint unglaubhaft, dass das BfV nicht in Lage gewesen sein soll, ein Testset hierfür zu entwickeln. Eine solche Möglichkeit müsste zumindest ernsthaft in Betracht gezogen und glaubhaft versucht werden. Dass keine gesetzliche Grundlage und auch keine Genehmigung der G 10-Kommission für die Verwendung der echten Daten vorlagen, kann dies ebenso wenig entschuldigen, wie eine etwaige Ausnahmegenehmigung durch die Amtsleitung.[922]

Problematisch ist weiterhin, dass die Daten ursprünglich nicht für solche Schulungszwecke errhoben wurden. Eine Verarbeitung von Daten, die nach G 10-Anordnungen erfasst wurden, ist zwar prinzipiell möglich, stellt hier jedoch im Zusammenhang mit Schulungsmaßnahmen durch Mitarbeiter_innen anderer Nachrichtendienste eindeutig eine Zweckentfremdung dar. Das BfV ändert damit nicht nur eigenständig den Verwendungszusammenhang, sondern erhöht damit auch die Verfügbarkeit der personenbezogenen Daten. Damit entsteht auch ein ganz neues Gefahrenpotenzial mit

920) *Treuenfels*, Protokoll-Nr. 94 I, S. 27.

921) *Genkova*, Protokoll-Nr. 89 I, S. 104.

922) *Treuenfels*, Protokoll-Nr. 94 I, S. 27.; zur Autorisierung durch die Amtsleitung des BfV: Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der SPD vom 14. August 2013, Bundestagsdrucksache 17/14456, S. 21.

neuer Qualität und besonders hoher Relevanz. Eine Verarbeitung solcher Daten hätte sich folglich auch nach diesen Vorschriften zur Datenübermittlung richten müssen.

Der Zweck der Datenübermittlung darf nicht unvereinbar sein mit dem Zweck der Datenerhebung. Dies ist jeweils im Einzelfall zu prüfen. Eine Prüfung muss zudem sowohl vom BfV, als auch vom BND erfolgen. Ein pauschaler Zugriff auf das vom BfV verwendete Programm durch den BND, wäre ebenso rechtswidrig, wie eine Verwendung dieses durch die NSA. Dennoch legte das BfV bis zuletzt einen Ausschluss solcher Vorgehensweisen nicht plausibel dar. Vor dem Hintergrund der Ringtauschthese ist dies besonders problematisch.

bb) Ungereimtheit Nr. 2: Fehlende Abschottung

Die Bunderegierung bekräftigte stets, dass

> „XKEYSCORE sowohl im Test- als auch in einem möglichen Wirkbetrieb von außen und von der restlichen IT-Infrastruktur des BfV vollständig abgeschottet als „Stand-alone“-System betrieben [wird]. Daher könne ein Zugang amerikanischer Sicherheitsbehörden ausgeschlossen werden.“[923]

Dieser vermeintliche Ausschluss steht jedoch durch die Untersuchungen des Ausschusses mehr als in Frage, vor allem da der zweite Teil der Stellungnahme sich als erwiesen falsch herausstellte. So lautet der als Behauptung deklarierte Wunsch der Bundesregierung weiterhin:

> „Beim BND ist ein Zugriff auf die erfassten Daten oder auf das System XKEYSCORE durch Dritte ausgeschlossen, ebenso wie ein Fernzugriff.“[924]

923) Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der SPD vom 14. August 2013, Bundestagsdrucksache 17/14456, S. 22.

924) Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der SPD vom 14. August 2013, Bundestagsdrucksache 17/14456, S. 22.

Die Intention der beiden Kooperationspartner war auch erkennbar eine andere. So heißt es in von *Snowden* veröffentlichten Dokumenten:

> „NSA also has held several multilateral technical meetings with BND/BfV/NSA/CIA to introduce SIGDEV methodology and tradecraft to improve the BfV's ability to exploit, filter, and process domestic data accesses and potentially develop larger collection access points that could benefit both Germany and the U.S."[925]

> „Die NSA hat zudem mehrere multilaterale Zusammenkünfte von BND/BfV/NSA/CIA zu technischen Themen veranstaltet, in denen SIGDEV-Methoden und Spionagepraktiken vorgestellt wurden, um die Möglichkeiten des BfV in der Ausschöpfung, Filterung und Verarbeitung inländischer Datenzugänge zu stärken sowie potentiell größere Zugriffspunkte für Datensammlung zu schaffen, die sowohl Deutschland als auch den USA nützen könnten."[926]

Welches Ziel die NSA mit der Softwareübergabe verfolgte, wird hier deutlich: Das BfV soll lernen, die inländischen Datenströme vollends aufklären und abschöpfen zu können, damit sowohl BND als auch NSA auf eine größere Menge und vor allem zielgerichtet erfasster Daten zugreifen können.

cc) Ungereimtheit Nr. 3: Jahrelange Probezeit

Die Testphase des Programms, der sogenannte Proof of Concept, begann im September 2013 und war zunächst vom BfV für sechs Monate angelegt.[927] Doch nach diesen sechs Monaten wurde der Probebetrieb nicht eingestellt, sondern weitergeführt und das über Jahre hinweg. Vor der Überführung in den Wirkbetrieb sei eine Sicherheitsüberprüfung erforderlich gewesen. Die Zeugin *Monika Genkova*, IT-Sicherheitsbeauftragte im BfV, war für die Sicherheitsprüfung von XKEYSCORE ver-

925) Snowden-Dokument: Information Paper der NSA vom 17. Januar 2013, MAT A Sek-4/1i, Bl. 2.

926) MAT A Sek-4/1i, übersetzt vom Sprachendienst des Deutschen Bundestags.

927) *Genkova*, Protokoll-Nr. 89 I, S. 103.

antwortlich und berichtete, es habe ausführliche Bemühungen gegeben sicherzustellen, dass die Rechner, mit denen im BfV XKEYSCORE betrieben wurden, keinerlei Daten unbeabsichtigt ausleiteten.[928] Doch eine Testphase, die jahrelang andauert und zudem mit einer nicht unerheblichen Anzahl an echten personenbezogenen Daten aus G 10-Maßnahmen betrieben wird, ist keine Testphase mehr. Das BfV hat diese Zeit verstreichen lassen, ohne eine Entscheidung über die weitere Vorgehensweise zu treffen. Diese Nicht-Entscheidung war folgenreich, da sie aufgrund der Datenübermittlungen Grundrechtsverletzungen mit sich führte, und hätte vom BfV verhindert werden müssen.

So erklärte die die Zeugin *Genkova*, vor dem Ausschuss, dass der sogenannte Proof of Concept keine größeren Sicherheitsfragen beinhaltete. Im BfV wurde hauptsächlich nur die fachliche Eignung des Systems geprüft.[929]

Die Mitarbeiterin im BfV, *Doreen Delmdahl*, sagte vor dem Untersuchungsausschuss aus:

> „Aber man merkte, dass sie [die Version von XKEYSCORE] – dafür sind ja auch diese Tests da – für unsere Aufgabe nicht so zugeschnitten war, wie wir sie bräuchten“.[930]

Sie erklärte weiterhin:

> „Wir wissen nicht, was das Programm tatsächlich tut, wenn wir es zum Beispiel ans Internet anbinden“.[931]

Vor allem aber lag hierin auch ein erhbeliches Sicherheitsrisiko. Bis zum Ende dieser fachlichen Eignung war das Sicherheitskonzept nicht vollends ausgereift, was auch den erheblich langen Zeitraum der „Testphase“ erklärt.[932]

---

928) *Genkova*, Protokoll-Nr. 89, S. 100 f., 101, 110, 120 f.

929) *Genkova*, Protokoll-Nr. 89 I, S. 108.

930) *Delmdahl*, Protokoll-Nr. 86 I, S. 16.

931) *Delmdahl*, Protokoll-Nr. 86 I, S. 65.

932) *Genkova*, Protokoll-Nr. 89 I, S. 95.

Fehlendes Vertrauen in die Funktionsweise verbreitete sich unter den BfV-Mitarbeiter_innen und rief Befürchtungen über die Folgen einer Überführung in den Wirkbetrieb hervor. Die Mitarbeiter_innen hatten keinen umfassenden Überblick über das, „was gegebenenfalls die Software noch tun könnte, das abgefangen“ werden müsste.[933] Die Schlussfolgerung aus solchen Befürchtungen hätte jedoch die Einstellung der Verwendung von XKeyscore – zumindest in dieser Form – sein müssen, und nicht das jahrelange Fortsetzen von Datenverwendungen mittels dieser und unter Beisein von Mitarbeiter_innen anderer Nachrichtendienste.

In Folge der öffentlichen Debatte zu PRISM, im Juli 2013, sollen die Tests gestoppt, aber schon nach kurzer Zeit wieder aufgenommen worden sein.

Eine Testphase, die jahrelang andauert und zudem mit einer nicht unerheblichen Anzahl von echten personenbezogenen Daten aus G 10-Maßnahmen betrieben wird, ist keine Testphase mehr. Das BfV hat diese Zeit verstreichen lassen, ohne eine Entscheidung über die weitere Vorgehensweise zu treffen. Diese Nicht-Entscheidung war folgenreich, da sie aufgrund der Datenübermittlungen Grundrechtsverletzungen mit sich führte, und hätte vom BfV verhindert werden müssen.

d) Keine Information über Einsatz von XKEYSCORE an Fachaufsicht und PKGr

Auch im Fall von XKEYSCORE erfuhren die Kontrollgremien erst durch die Presse vom dazugehörigen Vertrag und der unerlaubten Weitergabe von Daten an BND und NSA innerhalb der gemeinsamen Workshops erfahren. Weder ein Mitglied des Parlamentarischen Kontrollgremiums, noch die Fachaufsicht, der bzw. die Bundesdatenschutzbeauftragte noch ein Regierungsmitglied wussten von der Vertragszeichnung mit der NSA, oder dem darauf folgenden Einsatz der Spähsoftware.[934]

Der frühere Bundesbeauftragte für den Datenschutz, *Peter Schaar* erklärte**,** dass er weder über ein Kompensationsgeschäft noch über einen Test mit Echtdaten informiert

---

933) *Delmdahl*, Protokoll-Nr. 86 I, S. 66.

934) *Zeit Online* vom 26. August 2015, „Suche NSA-Spionagesoftware, biete deutsche Daten“, http://www.zeit.de/digital/datenschutz/2015-08/xkeyscore-nsa-verfassungsschutz, abgerufen am 4. Juni 2017.

worden war. Dass das BfV die Spähsoftware überhaupt einsetzt, wurde ihm erst mitgeteilt, als er im Zuge der *Snowden*-Veröffentlichungen von sich aus nachfragte. Die Verheimlichung der Nutzung von XKEYSCORE deklarierte er als rechtswidrig.[935]

Auch das PKGr wurde nicht hinreichend informiert und musste erst explizit nachfragen. Erst dann, als die Vorwürfe im Jahr 2013 unübersehbar im Raum standen, erfolgte eine äußerst allgemeine Unterrichtung. Mitgliedern des PKGr zufolge wäre das Abkommen zwischen Nachrichtendiensten zweifelsfrei ein „Vorgang von besonderer Bedeutung“ i.S.v. § 4 Abs. 1 PKGrG gewesen gewesen, über den die Bundesregierung selbständig und ausreichend informieren muss.[936]

Über erste Sondierungen wurde das BMI angeblich Anfang 2012 informiert. Den Erhalt der Software bestätigte das BfV nach Angaben der Bundesregierung am 22. Juli 2013, nach dem sie am 17. und 18. Juni 2013 installiert wurde und seit dem 19. Juni 2013 zu Testzwecken zur Verfügung stand.[937] Einem Bericht des BMI an das PKGr ist jedoch zu entnehmen, dass dieses über den Einsatz von XKEYSCORE im BfV aus Presseberichten im Juli 2013 erfahren haben soll.[938]

Das BfV berichtete folglich nicht selbstständig, sondern erst auf Grund von Nachfragen in Folge der *Snowden*-Enthüllungen. Jedoch hätte die Rechtsaufsicht als die Fachaufsicht über das BfV hierüber bereits vor der Erstellung und Unterzeichnung der ToR informiert werden müssen.

Infolge der Verheimlichung der Maßnahmen und Absprachen durch das BfV war eine Befassung und Auseinandersetzung sowie jedwede Kontrolle der Praxis des BfV ausgeschlossen. In jedem Fall darf es nicht den Geheimdiensten überlassen werden, über

935) *Zeit Online* vom 26. August 2015, „Suche NSA-Spionagesoftware, biete deutsche Daten“, http://www.zeit.de/digital/datenschutz/2015-08/xkeyscore-nsa-verfassungsschutz, abgerufen am 4. Juni 2017.

936) *Zeit Online* vom 26. August 2015, „Suche NSA-Spionagesoftware, biete deutsche Daten“, http://www.zeit.de/digital/datenschutz/2015-08/xkeyscore-nsa-verfassungsschutz, abgerufen am 4. Juni 2017.

937) Mitteilung der Bundesregierung an den Bundestag vom 14. August 2013, BT-Drucksache 17/14560, S. 20 ff.; Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der SPD vom 14. August 2013, Bundestagsdrucksache 17/14456, S. 21.

938) Bericht des BMI an das PKGr vom 25. Juli 2013, MAT A BMI-1/10m_1, Bl. 288 (VS-NfD)

Umfang und Art des Einsatzes einer solch bedeutenden Software selbständig zu entscheiden. Die parlamentarische, fachliche und rechtliche Kontrolle muss frühzeitig greifen und die Umsetzung stets kontrollieren.

e) Unstimmigkeiten beim Datentransport des BfV von Köln nach Berlin

Neben der Frage nach Funktionsweise und Datenweitergabe hat sich der Ausschuss auch damit beschäftigt, wie der Transport der mittels XKEYSCORE analysierten Daten zwischen den BfV-Dienststellen in Köln und Berlin umgesetzt wurde. Zunächst gab es dafür die sogenannte „Turnschuhschnittstelle“[939]:anfangs wurden die G 10-Daten, die aus der G 10-Anlage des BfV in Köln exportiert wurden, per Kurier zur Bearbeitung mit XKEYSCORE nach Berlin transportiert, und dies nicht etwa durch einen BfV-eigenen Kurierdienst erfolgte, sondern in zwei von drei Fällen durch den BND.

[redacted]

[940]

939) *A. Sch.,* Protokoll-Nr. 77 II – Auszug offen, S. 21.

940) Erläuternde Stellungnahme des BfV zum allgemeinen Anlauf des Transports von G 10-Daten vom BfV-Standort in Köln zum BfV-Standort in Berlin, MAT A BfV-19 (Tgb.-Nr. 65/16 – VS-VERTRAULICH), S. 1, 2.

[redacted]

[941]

Nach Angaben des BfV erfolgten im Untersuchungszeitraum drei Transporte von G 10-Daten über die „Turnschuhschnittstelle“ von Köln nach Berlin. Bei allen drei traten, wie nachfolgend zu ersehen ist, Unstimmigkeiten auf.

(1) Transport 1

Ein erster Transport fand im Rahmen einer Dienstreise zu Fortbildungszwecken von zwei BfV-Mitarbeitern zur Schule für Verfassungsschutz in Hermerzheim vom 4. bis zu 7. Juni 2013 statt. Dazu wurden dem Ausschuss die entsprechenden Dienstreiseanträge, Dienstreiseabrechnungen sowie das Fahrtenbuch des genutzten Dienstwagens für den entsprechenden Zeitraum vorgelegt.[942] Den Dienstreiseanträgen ist mittelbar

941) Erläuternde Stellungnahme des BND zur Weiterleitung von Postsendungen aus Köln (BfV) nach Berlin (BfV), MAT A BND-56 (Tgb.-Nr. 66/16 – VS-VERTRAULICH), S. 1, 2.

942) MAT A BfV-19, Bl. 4-15 (VS-NfD) u. 16-18 (offen).

zu entnehmen, dass dieser Transport von G 10-Daten auf der Rückreise von Hermerzheim via BfV-Standort Köln am 7. Juni 2013 stattfand.

Ferner weist das Fahrtenbuch die zurückgelegten Entfernungskilometer auf dem Hin- und Rückweg aus sowie den Sachverhalt, dass das Fahrzeug zu Abschluss der Dienstreise gewaschen wurde. Im Gegensatz dazu liegen ausweislich der dem Ausschuss zugeleiteten Unterlagen keinerlei Dokumente über den entsprechenden Transport von Verschlusssachen (VS) vor.

Weder besteht ein Empfangsschein, aus dem hervorgeht, was genau wann vom BfV in Köln versandt wurde, noch eine Nachweisliste, in der entsprechend Zählerstand, Zielort und G 10-Taschennummer verzeichnet sind, geschweige denn sonstige Dokumente, in denen die Sendung bei Entgegennahme in Köln und Übergabe in Berlin quittiert wurden. Solche aber müssten bestehen, da für die Mitnahme von Verschlusssachen (VS) auf Dienstreisen nach § 24 Abs. 2 VSA die Regelungen der Anlage 6 Nr. 3 entsprechend gelten, sodass für die Versendung von STRENG GEHEIM oder GEHEIM eingestuften VS zwischen getrennt liegenden Gebäuden, die nicht zu einer Gebäudegruppe gehören, ein verschlossener VS-Transportbehälter mit Zählwerkschloss zu benutzen ist. Daher hat das BfV im vorliegenden Fall entweder dem Ausschuss Unterlagen vorenthalten oder einen sorgfaltswidrigen, nicht sicherheitskonformen Umgang mit VS gepflegt.

(2) Transport 2

Ein zweiter Transport galt einer USB-Festplatte mit im Zeitraum vom 7. bis 13. Oktober 2013 aufgespielten Daten. Laut BfV-Empfangsschein wurde diese am 21. Oktober 2013 in Köln abgesandt und handschriftlich quittiert in Berlin am 28. Oktober 2013 entgegengenommen.[943] Die Nachweisliste zum Empfangsschein des BfV weist diesen Transport mit der Taschennummer „554“, Zielort Berlin und Zählerstand „767“ unter dem Datum „24.10.13“ aus,[944] somit aus unerfindlichen Gründen drei Tage nach dem Absendedatum in Köln am Montag, dem 21. Oktober 2013.

943) Empfangsschein des BfV zu einem G 10-Transport im Oktober 2013, MAT A BfV-19, Bl. 1 (VS-NfD).

944) Nachweisliste des BfV zm Empfangsschein eines G 10-Transports im Oktober 2013, MAT A BfV-19, Bl. 2 (offen).

Von der BND-Unterdienststelle in Bonn wurde eine entsprechende Versandliste, in der die Posttasche unter der Bezeichnung „[redacted] (i.e. der Zählerstand) benannt wird, zur Versendung nach Pullach am „[redacted] erstellt und mit dem Datumsstempel „[redacted]“ als ausgehend versehen.[945] In der Versandliste der BND-Unterdienststelle Pullach ist die Sendung unter „[redacted] verzeichnet. Sie wurde am „[redacted]“ erstellt, aber erst am Montag nach dem Wochenende, erkenntlich am Datumseintrag „[redacted]“, als ausgehend versandt.[946] Laut BND-Kurierbuch, darin bezeichnet als „[redacted] (i.e. Taschennummer/Zählerstand), wurde sie in Berlin am selben Tag vom BfV in Empfang genommen.[947]

(3) Transport 3

Ein dritter Transport beinhaltete eine externe Festplatte mit im Zeitraum vom 18. bis 24. November 2013 aufgespielten Daten. Laut BfV-Empfangsschein wurde diese, dort identifiziert mit der Seriennummer: „[redacted]“, am 4. Dezember 2013 in Köln abgesandt und handschriftlich quittiert in Berlin am 10. Dezember 2013 entgegengenommen.[948] Die Nachweisliste zum Empfangsschein des BfV weist diesen Transport bestehend aus zwei Taschen mit dem Zielort Berlin aus. Tasche Nr. 1 trägt die Taschennummer „[redacted]“ mit dem Zählerstand „[redacted]“. Der Eintrag zum Zählerstand wurde dabei durch Überschreibung der letzten Ziffer aus zuvor „[redacted]“ abgeändert. Tasche Nr. 2 trägt die Taschennummer „[redacted]“ mit dem Zählerstand „[redacted]“. Beide Eintragungen tragen die Datumsangabe „[redacted]“,[949] somit das im Empfangsschein ausgewiesene Absendedatum in Köln am 4. Dezember 2013.

---

945) Versandliste des BND von Bonn nach Pullach vom 22. Oktober 2013, MAT A BND-56 (Tgb.-Nr. 66/16 – VS-VERTRAULICH), Bl. 1 (VS-NfD).

946) Versandliste des BND von Pullach nach Berlin vom 25. Oktober 2013, MAT A BND-56 (Tgb.-Nr. 66/16 – VS-VERTRAULICH), Bl. 2 (VS-NfD).

947) Kurierbuch des BND zu Übergabe am 28. Oktober 2013, MAT A BND-56 (Tgb.-Nr. 66/16 – VS-VERTRAULICH), Bl. 3 (VS-NfD).

948) Empfangsschein des BfV zu einem G10-Transport im Dezember 2013, MAT A BfV-19, Bl. 1 (VS-NfD).

949) Nachweisliste des BfV zum Empfangsschein eines G10-Transports im Dezember 2013, MAT A BfV-19, Bl. 3 (offen).

Von der BND-Unterdienststelle in Bonn wurde eine entsprechende Versandliste, in der die Posttaschen unter der Bezeichnung „[redacted]“ und „[redacted]“ (i.e. jeweils der Zählerstand) benannt werden, zur Versendung nach Pullach am „[redacted]“ erstellt und mit dem Datumseintrag „[redacted]“ als ausgehend versehen.[950] In der Versandliste der BND-Unterdienststelle Pullach, erstellt am „[redacted] , sind die Sendungen jeweils unter „[redacted]“ mit den Bezeichnungen „[redacted] und „[redacted]“ verzeichnet.[951] Laut BND-Kurierbuch, darin bezeichnet als „[redacted]“ und „[redacted]“ (i.e. jeweils Zählerstand/Taschennummer), wurden sie nach dem Wochenende am Montag, dem „[redacted]“, abgesandt und am selben Tag in Berlin vom BfV in Empfang genommen.[952]

Wie aber eine (!) externe Festplatte in Form von zwei (!) Transporttaschen befördert werden konnte, ist aus den dem Ausschuss zugeleiteten Unterlagen nicht ersichtlich. Zwar besteht prinzipiell die Möglichkeit, dass zufällig zwei G 10-Taschen zeitgleich von Köln nach Berlin versandt und transportiert wurden, von denen eine keine G 10-Daten zur Weiterverarbeitung mit XKEYSCORE enthielt. Doch hätte dann in Entsprechung zum Eintrag in der Nachweisliste ein ausgefüllter Empfangsschein vorliegen müssen, aus dem Rückschlüsse auf den tatsächlichen Inhalt der Sendung hervorgingen.

Auch in diesem Fall drängt sich der Eindruck auf, dass das BfV entweder dem Ausschuss Unterlagen vorenthielt oder aber ein maximales Sicherheitsproblem im Umgang mit VS und dem Geheimschutz hat.

(4) Fazit

Aus der dem Ausschuss vorgelegten Aktenlage ist ein direkter Nachweis, dass sich der BND im Rahmen des Transports Zugriff auf die aus der G 10-Anlage des BfV in Köln exportierten Daten verschafft hat, nicht zu entnehmen. Die Unstimmigkeiten im

---

950) Versandliste des BND von Bonn nach Pullach vom 3. Dezember 2013, MAT A BND-56 (Tgb.-Nr. 66/16 – VS-VERTRAULICH), Bl. 4 (VS-NfD).

951) Versandliste des BND von Pullach nach Berlin vom 6. Dezember 2013, MAT A BND-56 (Tgb.-Nr. 66/16 – VS-VERTRAULICH), Bl. 5 (VS-NfD).

952) Kurierbuch des BND zu Übergabe am 9. Dezember 2013, MAT A BND-56 (Tgb.-Nr. 66/16 – VS-VERTRAULICH), Bl. 6 (VS-NfD).

materiellen Geheimschutz und deren Häufung – Transport 1: vollständig undokumentiert; Transport 2: Nachweisliste mit Eintrag zum Zählwerkstand drei Tage nach dem Versand erstellt; Transport 3: Eintragung des Zählwerkstands im Empfangsschein abgeändert, eine Festplatte in zwei Transporttaschen versandt bzw. Dokumente vorenthalten – sowie der generelle Umstand, dass der Inlandsgeheimdienst BfV grundrechtsrelevante G 10-Daten durch den Auslandsgeheimdienst BND transportieren ließ, lassen dies zugleich jedoch auch nicht ausschließen.

VIII. BND-Selektoren: Abhören unter Freunden geht wunderbar

1. Rechtswidrige BND-Selektoren

a) Überwachungsziele

Der BND hat ausweislich der gesichteten Untersuchungsausschuss-Akten mit eigenen Selektoren die Telekommunikation zahlreicher Regierungs-, Ministerien-, Botschafts- und sonstiger öffentlicher Stellen sowie von EU-Institutionen, VN und ihrer Organisationen sowie Politiker_innen, Journalist_innen und Redaktionen überwacht.

So überwachte der BND ab 1999 bis jedenfalls Herbst 2006 weltweit mindestens 50 Telefon- und Faxnummern oder E-Mail-Adressen von Journalist_innen oder Redaktionen: u.a. einen belgischer Journalisten im Kongo, mehr als ein Dutzend Anschlüsse der britischen *BBC* in Afghanistan und in der Zentrale London, ferner Redaktionen des internationalen Programms *BBC World Service*, ein Anschluss der *New York Times* in Afghanistan, Mobil- und Satellitentelefon-Anschlüsse der Nachrichtenagentur *Reuters* in Afghanistan, Pakistan und Nigeria, ferner Nachrichtenagenturen aus Kuwait, dem Libanon oder Indien sowie Journalistenverbände aus Nepal und Indonesien[953]. Auch die Spiegel-Journalistin *Susanne Koelbl* in Afghanistan überwachte der BND 2006 ein halbes Jahr zielgerichtet; des BNDs anfänglicher Erklärungsversuch hierfür (nur zufälliger „Beifang“) stellte sich später als Lüge heraus[954].

Gleiches behauptete der BND über sein im Februar 2012 aufgezeichnetes Telefonat der ex-US-Außenministerin *Clinton* mit dem damaligen UNO-Generalsekretär *Kofi Annan* sowie eines Telefonats des Clinton-Nachfolgers *John Kerry* aus Nahost. Während der BND letzteren Mitschnitt – entgegen seiner Auswertungspraxis zuvor – gemäß Kanzleramts-Anordnung vom Sommer 2013 sogleich vernichtete, wurde der Clinton/Annan-Mitschnitt weisungswidrig noch länger aufbewahrt und herumgereicht[955].

953) Spiegel Online vom 24. Februar 2017 „BND bespitzelte offenbar ausländische Journalisten“, abrufbar unter http://www.spiegel.de/politik/deutschland/bnd-bespitzelte-offenbar-auslaendische-journalisten-a-1136134.html

954) Spiegel Online vom 24. Februar 2017 „BND bespitzelte offenbar ausländische Journalisten“, abrufbar unter http://www.spiegel.de/politik/deutschland/bnd-bespitzelte-offenbar-auslaendische-journalisten-a-1136134.html

955) Spiegel Online vom 18. August 2014 „Beifang im Netz“, abrufbar unter http://www.spiegel.de/spiegel/print/d-128743698.html

Ebenfalls gezielt überwachte der BND gemäß dem „Auftragsprofil der Bundesregierung“ (Stand 2009) mindestens bis Mitte 2014 die Telekommunikation des NATO-Bündnispartners Türkei[956]. Bis zum Oktober 2013 überwachte der BND TK-Anschlüsse in befreundeten Staaten: z. B. „in hunderten Fällen“ die Telekommunikation US-amerikanischer Außen- und Verteidigungspolitiker_innen sowie von Senator_innen, v.a. wenn diese unterwegs unverschlüsselt kommunizierten. Die Protokolle etwa während des Irak-Kriegs ließ der damalige BND-Chef *Hanning* auch dem Kanzleramt unterbreiten. Erst als die Kanzlerin (auf die US-Überwachung ihres eigenes Handies bezogen) öffentlich sagte „Abhören unter Freunden, das geht gar nicht“, schaltete die BND-Spitze und ließ flugs rund 2800[957] entsprechende Selektoren dieser Personengruppe löschen[958]. Außerdem ließ der BND die iranische Botschaft im EU-Partnerland Österreich abhören, ferner mehrere französische Botschaften: angeblich um so deren Infos über Afghanistan oder nordafrikanische Staaten zu erlangen, statt erstere direkt zu fragen[959]. Angeblich wies Ex-BND-Präsident *Schindler* im März 2014 ändernd an, Komunikation befreundeter Politiker_innen doch wieder zu überwachen und zu verwenden, wenn sie mit jemand von Interesse für den BND sprächen. Dem zuständigen Parlamentarischen Kontrollgremium des Bundestages log die Bundesregierung auf vielfache Fragen hin zwei Jahre lang die „Beifang“-Erklärung vor und offenbarte den realen Umfang der tatsächlich gezielten BND-Überwachung solcher Ziele erst Mitte Oktober 2015[960].

---

956) *Spiegel Online* vom 18. August 2014 „Beifang im Netz“, abrufbar unter http://www.spiegel.de/spiegel/print/d-128743698.html

957) 3.300 laut öffentlicher Bewertung des PKGr (Mehrheit) vom 16. Dezember 2015, abrufbar unter https://www.bundestag.de/dokumente/textarchiv/2015/parlamentarisches-kontrollgremium/399586; Bundestagsdrucksache 18/9142: wohl 2/3 der Ende 2015 noch nachvollziehbaren 40.000 BND-Selektoren seien demnach rechts- bzw. auftragswidrig gewesen. Dagegen Minderheitsvotum MdB Ströbele (schriftliche Version vom 30. Dezember 2015): all diese 40 000 waren rechtswidrig, sonst hätten BND-Spitze sie nicht initiativ entfernen lassen!, abrufbar unter http://www.stroebele-online.de/show/8838258.html

958) *Süddeutsche Zeitung Online* vom 15. Oktober 2015 „Wie der BND seine Spähaktionen vertuschen wollte“, abrufbar unter http://www.sueddeutsche.de/politik/geheimdienst-wie-der-bnd-seine-spaehaktionen-vertuschen-wollte-1.2693574

959) *Süddeutsche Zeitung Online* vom 15. Oktober 2015 „Wie der BND seine Spähaktionen vertuschen wollte“, abrufbar unter http://www.sueddeutsche.de/politik/geheimdienst-wie-der-bnd-seine-spaehaktionen-vertuschen-wollte-1.2693574

960) *Süddeutsche Zeitung Online* vom 15. Oktober 2015 „Wie der BND seine Spähaktionen vertuschen wollte“, abrufbar unter http://www.sueddeutsche.de/politik/geheimdienst-wie-der-bnd-seine-spaehaktionen-vertuschen-wollte-1.2693574

Außerdem überwachte der BND spätestens seit 2000 jahrelang Telefon- und Faxnummern sowie Mailadressen des internationalen Polizeinetzwerks Interpol (deren Zentrale in Lyon, Verbindungsbüros des Polizeinetzwerks in Österreich, Dänemark, Belgien, Griechenland, Spanien, Italien, USA und Dutzenden weitere Staaten) sowie der europäischen Polizeibehörde Europol in Den Haag[961].

Der BND schaltete Überwachungs-Selektoren (z.B. E-Mail-Adressen, Telefon-und Telefaxnummern) gegen ‚fast alle europäischen Botschaften' und zahlreiche Konsulate in Deutschland bis zu einer Vertretung des Vatikan, ferner der Innenministerien in Wien und Brüssel, des Verteidigungsministeriums in London, des Außenministeriums der USA, außer von Banken wie der *HSBC*, Internationale Institutionen (z. B. das UN-Drogenkontrollprogramm, OSZE in Wien, Opec, der IWF in Washington), Nichtregierungsorganisationen (z.B. Oxfam, Care International, das Internationale Komitee vom Roten Kreuz in Genf, das International Medical Corps in Los Angeles, der International Action Center in New York), Büros von Politiker_innen (z.B. des israelischen Ministerpräsidenten; ab 2009 mehrjährig EU-Repräsentantin Außen- und Sicherheitspolitik sowie Vizepräsidentin der EU-Kommission *Catherine Ashton*, den EU-Außenminister *John Kerry* ab 2013 per Mobil- und Büro-Nummern[962], den französischen Ex-Außenminiuster *Laurent Fabius*[963]), Telekommunikationsunternehmen (wie *British Telecommunications*, *MCI Worldcom*), ein Flugzentrum der Nasa, eine Niederlassung der U. S. Air Force, zahlreiche mittelständische Unternehmen in Österreich und der Schweiz, selbst *Heckler & Koch* in Baden-Württemberg (damals in britischem Besitz)[964]. Der BND überwachte die Firmen *Eurocopter* und *EADS* nicht nur im Auftrag der NSA (73 TK-Anschlüsse bis 2006), sondern auch höchstselbst mindestens zwei Niederlassungen in Polen und Warschau[965]. Insgesamt hatte der BND zigtausende Selektoren für die NSA geschaltet (und dies laut internen Akten des PUA schon 2008 einem Kanz-

961) Vgl. *Der Spiegel* vom 22. April 2017 S. 21.

962) *Spiegel Online* vom 27. Februar 2016 „Abhören von Freunden – geht gut", abrufbar unter http://www.spiegel.de/spiegel/print/d-143351295.html.

963) *Die Welt* vom 13. November 2015, „Warum der BND einen Deutschen ausspähte".

964) *Spiegel Online* vom 2. April 2016, „Die Fleurop-Liste", http://www.spiegel.de/spiegel/print/d-143908100.html.

965) *Spiegel Online* vom 2. April 2016, „Die Fleurop-Liste", http://www.spiegel.de/spiegel/print/d-143908100.html.

leramts-Referatsleiter berichtet), wovon er rd. 40.000 seit 2013 sukzessiv aussson-derte (davon 68,7 % gegen EU-Regierungsstellen und viele weitere gegen deutsche Firmen)[966]. Der BND überwachte mit eigenen Selektoren auch Deutsche Staatsbürger_innen (z. B. Mitarbeiter_innen in ausländischen EU-Einrichtungen oder Diplomat_innen wie den Gatten der BMI-Staatssekretärin *Emily Haber*, *Hansjörg Haber*, als dieser 2008 bis 2011 die EU-Beobachtermission in Georgien leitete)[967].

Daß der BND so erlangte Rohdaten sehenden Auges gegen deutsche / europäische Interessen an die NSA übermittelte – ab 2002 sogar automatisiert –, versuchte er mit internen „Gutachten" zu rechtfertigen: Die „willentliche Weitergabe" solcher Daten sei zwar „rechtswidrig", doch bemühe sich der BND ja immerhin, deutsche Staatsbürger_innen herauszufiltern (allerdings mit erkannt untauglichen Filtern). Es sei daher rechtlich „nicht zu beanstanden", wenn der automatische Datenaustausch „als höherwertig anzusehen ist" als die vereinzelte Weitergabe von „Erkenntnissen zu deutschen Staatsangehörigen"[968].

b) Rechtswidrigkeit der BND-eigenen Steuerung in der strategischen Fernmeldeaufklärung

Die BND-eigene Steuerung in der strategischen Fernmeldeaufklärung ist rechtswidrig. Sie greift in ungerechtfertigter Weise in den Schutzbereich des Art. 10 GG, also des Fernmeldegeheimnisses ein. Steuerung umschreibt ganz technisch, dass personenbezogene Telekommunikationsmerkmale für das Ausfiltern von Daten wie Mails, Telefongespräche, SMS usw. als Auswahlkriterien verwendet werden. Der Schutzbereich des Art. 10 GG ist auch für ausländische Kommunikationsteilnehmer im Ausland eröffnet. Zwar hat das Bundesverfassungsgericht in seiner Entscheidung zur Antiterrordateigesetz[969] weder behandelt noch explizit festgestellt, dass diese Personengruppe ebenso wie deutsche Staatsbürger_innen als Träger_innen von Grundrechten im

966) *Spiegel Online* vom 2. April 2016 „Die Fleurop-Liste", abrufbar unter http://www.spiegel.de/spiegel/print/d-143908100.html; sogen. „Gruppenliste" in Datenbank der BND-Abt. TA vgl. PKGr-Bericht in Bundestagsdrucksache 18/0142 vom 7. Juli 2016, abrufbar unter https://dipbt.bundestag.de/doc/btd/18/091/1809142.pdf.

967) *Spiegel Online* vom 2. April 2016 „Die Fleurop-Liste", http://www.spiegel.de/spiegel/print/d-143908100.html.

968) *Spiegel Online* vom 2. April 2016 „Die Fleurop-Liste", http://www.spiegel.de/spiegel/print/d-143908100.html.

969) BVerfGE 133, 277 (325) Rdnr. 117 f.

Sinne des Art. 10 GG geschützt sei. Die Auffassung des BND aber, beim Fernmeldegeheimnis des Art. 10 GG handele es sich um ein Grundrecht nur deutscher Staatsbürger_innen und die reine Auslandsaufklärung des BND (nur bzgl. Kommunikationsverkehren von Ausländer_innen, die sich im Ausland befinden) greife daher in dieses Grundrecht nicht ein, trägt nicht. Vielmehr gilt: Ist ein Kommunikationsvorgang sachlich von Art. 10 GG umfasst (also u.a. jeder „Fernmelde“-Verkehr), so kann es auf die Staatsangehörigkeit der jeweiligen Kommunikationsteilnehmer_innen nicht ankommen.[970]

Auch die durch den BND entwickelte „Funktionsträgertheorie“ zur weiteren Eingrenzung des persönlichen Schutzbereichs des Art. 10 GG lässt sich nicht halten.

Nach der „Funktionsträgertheorie“ sollen auch deutsche Staatsbürger_innen im Ausland durch Suchbegriffe in ihrer engsten Privatsphäre oder gezielt an ihren Telekommunikationsanschlüssen überwacht werden dürfen (Ausnahme gemäß § 5 Abs. 2 S. 3 Artikel 10-Gesetz), wenn sie im Ausland für ein ausländisches Unternehmen oder eine ausländische Organisation kommunizieren. Ihre Kommunikation sei – da sie lediglich Funktionsträger_innen der ausländischen juristischen Person sind – auch nur dieser zuzuordnen. Da ausländischen juristischen Personen jedoch gemäß Art. 19 Abs. 3 GG nicht den Schutz des Fernmeldegeheimnisses genießen, könne Art. 10 GG auch ihre Funktionsträger_innen nicht schützen.

Bei dieser Funktionsträgertheorie des BND handelt es sich um nichts weniger als die bewusste Umgehung des verfassungsrechtlich gewährleisteten Grundrechtsschutzes. Ihr fehlt jegliche gesetzliche oder rechtliche Grundlage. Das Fernmeldegeheimnis schützt primär die Kommunikationsteilnehmer_innen selbst, der Grundrechtsschutz

---

970) *Bäcker,* „Der BND baut sich einen rechtsfreien Raum: Erkenntnisse aus dem NSA-Untersuchungsausschuss“, abrufbar unter http://verfassungsblog.de/der-bnd-baut-sich-einen-rechtsfreien-raum-erkenntnisse-aus-dem-nsa-untersuchungsausschuss/.

der juristischen Personen im Inland und EU-Ausland wird faktisch über diese vermittelt.[971] So bleibt der Grundrechtsschutz der kommunizierenden natürlichen Person natürlich auch bestehen, wenn sie für eine ausländische juristische Person kommuniziert. Die Funktionsträgertheorie käme zudem einem verfassungswidrigen Verlust der Grundrechte gleich, wenn man für eine ausländische juristische Person arbeitet und für diese kommuniziert. Eine Trennbarkeit der Kommunikation als natürliche Person und derjenigen als Funktionsträger_in einer ausländischen juristischen Person ist im Übrigen kaum möglich. Dies insbesondere dann nicht, wenn es sich um eine breiter angelegte, personalisierte Steuerung geht. Der Schutz der Menschenwürde und des Fernmeldegeheimnisses als Jedermann-Grundrecht findet insofern auch für die Bespitzelung ausländischer Funktionsträger_innen Anwendung.

Die Konstruktion eines quasi rechtsfreien Raumes durch die Funktionsträgertheorie für BND-eigene Steuerung in der strategischen Fernmeldeaufklärung lässt sich nicht halten[972]. Die Steuerung durch Selektoren greift in den Schutzbereich des Art. 10 GG ein, ohne dass diese durch eine G 10-Anordnung gerechtfertigt wäre.

c) Steuerung von Regierungen, Ministerien, Botschaften und sonstigen öffentlichen Stellen; EU Institutionen, VN und ihre Organisationen rechtswidrig

Da es sich – wie dargelegt – bei Art. 10 GG um ein Jedermann-Grundrecht handelt und die Funktionsträgertheorie sich nicht aufrechterhalten lässt, war auch die Steuerung von Regierungen, Ministerien, Botschaften und sonstigen öffentlichen Stellen, EU Institutionen, den Vereinten Nationen und ihren Organisationen ein ungerechtfertigter Eingriff in das Fernmeldegeheimnis der Kommunikationsteilnehmer, soweit er ohne eine G 10-Anordnung erfolgte.

---

971) *Bäcker,* „Der BND baut sich einen rechtsfreien Raum: Erkenntnisse aus dem NSA-Untersuchungsausschuss“, abrufbar unter http://verfassungsblog.de/der-bnd-baut-sich-einen-rechtsfreien-raum-erkenntnisse-aus-dem-nsa-untersuchungsausschuss/.

972) Dagegen auch BfDI *Voßhoff*, Stellungnahme von Mitte Februar 2016 an die G10-Kommission („nicht verfassungskonform“, „überkommene Vorstellung des BND: Im Zweifel für die Erfassung“ statt gehörig „Im Zweifel für den Grundrechtsschutz“. Art. 10 GG mache „keinen Unterschied“ zwischen privater, geschäftlicher oder politischer Kommunikation); zitiert nach Süddeutsche Zeitung Online vom 24. Februar 2016, abrufbar unter http://www.sueddeutsche.de/politik/geheimdienst-abhoerpraxis-des-bnd-nicht-verfassungskonform-1.2878299.

Die Steuerung von Staats- und Regierungschefs aus EU- und NATO-Ländern verstieß zudem gegen Sinn und Wortlaut der EU- und NATO-Verträge, die auf Vertrauen und Solidarität der Partner aufgebaut sind. So heißt es in der Präambel der EU-Verträge:

> „SCHÖPFEND aus dem kulturellen, religiösen und humanistischen Erbe Europas, aus dem sich die unverletzlichen und unveräußerlichen Rechte des Menschen sowie Freiheit, Demokratie, Gleichheit und Rechtsstaatlichkeit als universelle Werte entwickelt haben, […]
>
> IN DEM WUNSCH, die Solidarität zwischen ihren Völkern unter Achtung ihrer Geschichte, ihrer Kultur und ihrer Traditionen zu stärken, […]
>
> HABEN [die Mitgliedstaaten der EU] BESCHLOSSEN, eine Europäische Union zu gründen“[973]

Aber auch der NATO-Vertrag mit seiner Verpflichtung zum gegenseitigen Beistand beinhaltet in besonderer Weise den Ausdruck des völkerrechtlichen Prinzips von Treu und Glauben (good faith), wie es in Art. 26 der Wiener Vertragsrechtskonvention niedergelegt ist. Hieraus ergibt sich unter den NATO-Partnern eine besondere Loyalitäts-Verpflichtung in den zwischenstaatlichen Beziehungen, welcher die Steuerung der Regierungen der Vertragspartner widerspricht.[974]

Sie stellt weiterhin einen Verstoß gegen das Prinzip der souveränen Gleichheit der Staaten (Art. 2 Nr. 1 VN-Charta) dar, da Regierungskommunikation genuiner Teil der inneren Angelegenheiten eines Staates (domaine réservée) ist.[975]

---

973) Präambel des Vertrags über die Europäische Union.

974) Vgl. auch: Gewinnung von Telekommunikationsinformationen durch ausländische Nachrichtendienste aus völkerrechtlicher Sicht, WD 2 – 3000 – 083/13, S. 12.

975) Gewinnung von Telekommunikationsinformationen durch ausländische Nachrichtendienste aus völkerrechtlicher Sicht, WD 2 – 3000 – 083/13, S. 6.

Die Überwachung von ausländischen Botschaften in Deutschland stellte zudem einen direkten Verstoß gegen das Völkerrecht dar. Gemäß Art. 27 Abs. 1 des Wiener Übereinkommens über diplomatische Beziehungen gestattet und schützt der Empfängerstaat den freien Verkehr für alle amtlichen Zwecke. Absatz 2 wird noch deutlicher:

> „Die amtliche Korrespondenz der Mission ist unverletzlich. Als „amtliche Korrespondenz“ gilt die gesamte Korrespondenz, welche die Mission und ihre Aufgaben betrifft.“

Das Abfangen der Kommunikation der ausländischen diplomatischen Vertretungen in der Bundesrepublik stellte damit einen klaren Verstoß gegen den Wortlaut des Wiener Übereinkommens dar.

Es ist nicht abwegig, dass auch die Überwachung ausländischer diplomatischer Vertretungen im Ausland durch den BND gegen das Völkerrecht oder das Völkergewohnheitsrecht verstieß.

2. Kontrollfreier Raum der Technischen Aufklärung

Die Beweisaufnahme hat hinsichtlich der BND-eigenen Steuerung vergleichbare Defizite aufdecken können wie in der Zusammenarbeit mit der *NSA*. Allerdings konnte der Ausschuss in diesem Zusammenhang deutlich tiefer in die Materie vordringen, da den Mitgliedern auch Selektoren selbst vorgelegt wurden. Ob dies alle rechtswidrig gesteuerten Selektoren waren, hat der Untersuchungsausschuss nicht überprüfen können. Vielmehr musste sich der Ausschuss auf die ihm unter besonderen Geheimschutzauflagen zugänglich gemachten Unterlagen beschränken. Weitere Anhaltspunkte hatte zudem auch der Bericht des Parlamentarischen Kontrollgremiums (PKGr) vom 7. Juli 2016 geliefert.[976]

a) Das Gras wachsen hören

Die gängige Erläuterung von *Kanzleramt* und *BND* in der Vergangenheit, bspw. beim Ausspähen auch deutscher Journalist_innen war immer wieder, dass es sich dabei

976) Bundestagsdrucksache 18/9142

lediglich um unbeabsichtigten „Beifang“ handeln würde. Die vorgelegten Beweismaterialien und die gehörten Zeugen ergaben ein anderes Bild. Ausgangspunkt dafür war ein Bericht des Magazins *Der Spiegel* vom 15. Oktober 2015.[977]

Mehrfach haben Zeugen betont, dass Ausgangspunkt für die Tätigkeit einer Vielzahl verschiedener Sachbearbeiter insbesondere auch in den Außenstellen des BND lediglich das Auftragsprofil der Bundesregierung (APB) oder eine sogenannte Kurzfristige Auftragssteuerung (KAST) gewesen sei. Allerdings hat es dabei keinerlei Kontrolle gegeben. Nachdem der Ausschuss zunächst nur eingeschränkte Informationen erhalten hatte, erhielten die Parlamentarier_innen in Folge des Erweiterungsbeschlusses zum PUA-Auftrag umfangreiche Unterlagen zur Einsicht einschließlich aussortierter BND-Selektoren.

Das Bundeskanzleramt und der BND haben im Zuge der Zeugenvernehmungen versucht, die Legende herzustellen, dass der BND in Gestalt des Unterabteilungsleiters *D. B.* bereits vor den Veröffentlichungen von *Edward Snowden* versucht habe, die Probleme in der eigenen BND-Steuerung in den Griff zu bekommen. Aktenkundige Belege dafür gibt es nicht. Vielmehr wurde deutlich, dass bereits im Jahr 2009 eine Weisung über das Verbot der gezielten Erfassung von Telekommunikationsverkehren von UN- und EU-Partnern in der Abteilung TA für „Unruhe“ bei den Sachbearbeiter_innen geführt habe. In einem entsprechenden Vermerk wurde aber innerhalb der Abteilung TA für den Bereich der strategischen Fernmeldeaufklärung u.a. im Kabelbereich klargestellt, dass das Kanzleramt diesen Bereich nicht mit seiner Weisung erfasst haben wolle, da es dies nicht ausdrücklich in seiner Weisung von 2008 erklärt habe.[978] Die vorhandenen Unterlagen über die von dem Zeugen *D. B.* angeblich schon im Frühjahr 2013 in Auftrag gegebene Handreichung oder „Matrix“ zur Einsteuerung von Zielen von Partnern datieren erst von Juli 2013 und damit eindeutig nach den Veröffentlichungen von *Edward Snowden*.

977) *Spiegel Online* vom 15. Oktober 2015 „BND spionierte europäische und US-Ziele aus“, abrufbar unter http://www.spiegel.de/politik/deutschland/bnd-spionierte-usa-und-andere-partnerlaender-aus-a-1057851.html

978) U. a. *D. B.*, Protokoll-Nr. 112 I, S. 27; *B. R.*, Protokoll-Nr. 126 II – Auszug offen, S.168 f.

Aufällig ist in diesem Zusammenhang, dass zum einen auch betont wurde, dass der BND die Erfassungsergebnisse aus den NSA-Selektoren durchaus auch für sich verwandt habe, soweit sich daraus ein entsprechender Mehrwert für den Dienst ergebe. Gleichzeitig wurde behauptet, dass die NSA-Selektoren erst im Sommer 2013 nach den Veröffentlichungen von *Snowden* näher untersucht worden wären. Der Zeuge *B. R.* hat zudem ausdrücklich bestätigt, dass er erst im Juli 2013 begonnen habe, Selektoren aus der BND-eigenen Steuerung zu deaktivieren, um die Erfassung von EU- und Nato-Zielen zu verhindern.[979] Unabhängig von diesen Arbeiten soll nahezu parallel der Zeuge *Dr. T.* das Steuerungsprofil der NSA untersucht haben, ohne dass diese Prozesse miteinander in Verbindung gestanden hätten.

Deutlich geworden ist, dass nahezu in jeder Außenstelle und in der Zentrale Selektoren für die eigene Steuerung des BND kreiert und eingestellt wurden. Die Zuordnung zu relevanten Phänomenbereichen scheint eher willkürlich erfolgt zu sein. Insbesondere war nicht nachvollziehbar, auf welcher Grundlage und mit welchem kenntnisstan die jeweiligen Telekommunikationsmerkmale ausgesucht, dem jeweiligen Phänomenbereich zugewiesen und auf Erforderlichkeit und Geeignetheit für die Aufgabenerfüllung des BND geprüft wurden.

Teilweise sind dem Ausschuss Telekommunikationsmerkmale vorgelegt worden, die über einen Zeitraum von mehreren Jahren eingesteuert waren. Dass damit relevante Informationen erfasst worden wären, war demgegenüber nicht oder nicht immer feststellbar. Teilweise war nicht einmal feststellbar, welchem Phänomenbereich die Telekommunikationsmerkmale zugeordnet waren. Anhaltspunkte dafür, dass die Merkmale vor ihrer Einsteuerung oder nach Ablauf eines bestimmten Zeitraums in der Steuerung auf die Notwendigkeit und Erforderlichkeit betrachtet wurden, waren nicht feststellbar.

Soweit sich der BND – wie schon zuvor gegenüber dem Parlamentarischen Kontrollgremium – auf verschiedene rechtliche Gründe gestützt hat, konnte dies im Ergebnis nicht überzeugen.

979) *B. R.*, Protokoll-Nr. 126 II – Auszug offen, S. 49

So war beipielsweise bei Angehörigen von Institutionen der Vereinten Nationen, der Europäischen Kommission, des Europarates oder ähnlicher Institutionen nicht erkennbar, dass die Überwachung deren elektronischer Telekommunikation überhaupt nicht anders zu erlangende Erkenntnisse im Rahmen des Aufgabenprofils hätten erbringen können. Gleiches galt für die Überwachung von EU-Bürger_innen oder Behörden bzw. Regierungseinrichtungen in Partnerstaaten. Teilweise war auch für den BND nicht mit letzter Sicherheit nachvollziehbar oder rekonstruierbar, warum es zu den Steuerungen über teils mehrjährige Perioden gekommen war. Besonders augenfällig wurde dies, wenn lediglich Bestandteile eines Telekommunikationsmerkmals Verwendung fanden, so dass die Anzahl gleichzeitig betroffener Telekommunikationsteilnehmer exponentiell ansteigen musste.

Die im öffentlichen Bericht des PKGr vom 7. Juli 2016[980] dargestellten Beispiele vermitteln ein anschauliches Bild, aber weder eine abschließende noch repräsentative Darstellung. Angesichts der Einstufung der entsprechenden Inhalte wird auf nähere Spezifizierungen verzichtet.

Dass es nahezu allen Sachbearbeiter_innen allein auf Basis einer großzügigen Auslegung des APB möglich war, eine langjährige Einsteuerung von rechtswidrigen Telekommunikationsmerkmalen in die Aufklärungssysteme des BND, insbesondere in seine Außenstellen, zu besorgen, bestätigt die während der Ausschussarbeit bereits offenbar gewordene „Blauäugigkeit“. Dass die Einsteuerung von Telekommunikationsmerkmalen zu europäischen Bürger_innen und Institutionen gegen Gemeinschaftsrecht und die Europäische Menschenrechtskonvention verstieß, ist vom BND geflissentlich unberücksichtigt geblieben. Die auch von Verfassung wegen notwendigen Grundsätze für die Datenerhebung wurden ersichtlich nie für die praktische Arbeit des BND bei der Datenverarbeitung herangezogen.

Soweit im Zusammenhang mit der Arbeit des Ausschusses die sogenannte „Weltraumtheorie“[981] eine gewisse Bekanntheit erlangt hat, sind entsprechende Überlegungen

980) Bundestagsdrucksache 18/9142, S. 8 ff.

981) Vgl. „Weltraumtheorie“ in Kapitel V.9.a)gg)aaa) – Datenübermittlungen des BND an die NSA aus Bad Aibling

oder Grundsätze jedenfalls durch den handelnden Sachbearbeiter wohl eher nicht angewendet worden. Der Horizont der rechtlichen Zulässigkeitsprüfung endete eher dabei, dass möglichst keinerlei Verletzung des engen G-10-Schutzbereichs im *BND* verursacht bzw. bejaht werden sollte. Weitergehende Überlegungen wurden nicht angestellt, sondern insbesondere die Eigenschaft der Abteilung TA als bloße Auftragnehmerin betont und die Verantwortung der politischen Ebene der Bundesregierung zugewiesen. Denn diese sei schließlich Auftraggeberin und verantwortlich für das APB.

Tatsächlich haben sowohl das übergeordnete Bundeskanzleramt als auch die Leitungsebene des BND versäumt, jemals mit Anweisungen oder dezidierten Vorgaben die Arbeit der Abteilung TA und damit die BND-eigene Steuerung im von Verfassung und europa- bzw. völkerrechtlichen Normen und Vereinbarungen gesteckten Rahmen zu lenken. Soweit das Kanzleramt der Abteilung TA ein Eigenleben unterstellte, lenkte es vom eigenen anscheinend planvollen Nichthandeln ab. Die Legitimation und Befürwortung der Erfassungsmaßnahmen ohne das reguläre Verfahren hat seinerseits den Schutzbereich des Artikels 10 GG aushölen geholfen. Darin lies sich ein beachtliches Eigenleben entwickeln, ersichtlich befürwortet vom Kanzleramt. Dieses trägt deshalb auch die Verantwortung für die begangenen Rechtsverstöße.

IX. „No Spy" und Pofallas Erklärung

1. Pofallas Erklärung vom 12. August 2013

Die Bundesregierung zog am 12. August 2013 die Notbremse, nachdem sie in den Sommermonaten vergeblich versucht hatte, die Vorwürfe aus den Veröffentlichungen der Snowden-Dokumente abzuwehren. Einen Monat vor der Bundestagswahl 2013 versuchte sie alles Belastende vom Tisch zu räumen. Kein geringerer als der Chef des Bundeskanzleramtes, Staatsminister *Pofalla*, selbst verlas im Anschluss an eine Sitzung des streng abgeschirmt und geheim tagenden Parlamentarischen Kontrollgremiums des Bundestages überraschend eine vorbereitete schriftliche vierseitige Erklärung mit dem Ergebnis der Sitzung des Gremiums.

Gleich an sechs Textstellen des Papiers wird versichert, die Geheimdienste der USA (NSA) und Großbritanniens (GCHQ) hätten mitgeteilt, dass sie „Recht und Gesetz in Deutschland einhalten". Die NSA unternehme auch nichts, um deutsche Interessen zu schädigen. Die US-Seite habe sogar den „Abschluss eines No-Spy-Abkommens angeboten", das stilbildend für die westlichen Dienste sein könne.

Nichts davon war richtig und stimmte. Ihren Zweck hatte die Wahlkampfaktion des Kanzleramts gleichwohl erreicht. BND und NSA waren bis zur Wahl und dem Bekanntwerden des Abhörens der Kanzlerin Handy aus den Schlagzeilen.

a) Weder ein „Angebot" noch ein No-Spy-Abkommen

Heute wissen wir, es gab kein „Angebot" der US-Seite für ein „No-Spy-Abkommen". Was es bei den Gesprächen in den USA vom 4. bis 6. August 2013 vermutlich gegeben hat, waren Überlegungen der US-Gesprächspartner_innen aus den Nachrichtendiensten zu Grenzen und Grundsätzen nachrichtendienstlicher Überwachung. Die Beweisaufnahme hat ergeben, dass am 5. August 2013 die deutsche Delegation in Washington auf die US-Nachrichtendienstchefs *Clapper* und *Alexander* trafen. In diesem Gespräch soll *Clapper* gesagt haben, es könne sich die Bildung einer Arbeitsgruppe vorstellen, die ein Abkommen nach dem Vorbild des MoA aus dem Jahr 2002 für ganz Deutschland erarbeite. Seinerzeit war vereinbart worden, dass beide Seiten sich an deutsches Recht und Gesetz halten. *Clapper* soll auch betont haben, er könne nichts entscheiden, dies könne nur die US-Regierung. Der Zeuge BND-Präsident *Schindler*

meinte sich zu erinnern, die Worte „No-Spy“ seien gefallen. Andere Teilnehmer dieses Gesprächs, die Zeugen *Fritsche* und *Heiß*, bestätigten nicht, dass diese Worte in der Besprechung vorkamen. Jedenfalls soll es Vorbehalte der USA gegen eine Vereinbarung gegeben haben und klargestellt worden sein, über das Ob einer solchen entscheide allein die politische Ebene – sprich: die Regierung.

Dies wurde nachträglich bestätigt, als nach *Pofallas* Erklärung Anfang November 2013 BND-Präsident *Schindler* erneut in die USA reiste und dort NSA-Direktor *Alexander* traf. Dieser wies erneut auf die Notwendigkeit einer Genehmigung durch die US-Regierung für jegliche Vereinbarung hin.

Von einem solchen Vorbehalt und der Notwendigkeit einer Entscheidung der Regierungsebene ist in der Erklärung *Pofallas* vom 12. August 2013 überhaupt keine Rede. Vielmehr wird gezielt der Eindruck erweckt, als sei es nur noch eine Frage einzelner Formulierungen, bis das „No-Spy-Abkommen“ steht und unterzeichnet werden kann.

In den folgenden Tagen verkündete auch der Regierungssprecher *Seibert*, es werde ein „No-Spy-Abkommen“ geben. Der damalige Innenminister *Friedrich* verstieg sich in der „*Rheinischen Post*“ wenige Tage nach *Pofallas* Auftritt gar zu der Behauptung, noch vor der Bundestagswahl werde eine Vereinbarung unterzeichnet, wonach die USA „uns als befreundete Nation nicht ausspionieren“.[982] Das führte zu erheblicher „Verwunderung“ in der US-Botschaft und zur Mahnung, die öffentliche Debatte unter Kontrolle zu halten.[983] Ein weiteres Indiz dafür, worum es der Bundesregierung eigentlich ging: Nämlich um die bevorstehende Bundestagswahl einen Monat später.

Schon gar nicht ergab sich aus Verhandlungen des Auswärtigen Amtes Ende Juli, Anfang August 2013 und in den Monaten danach mit den US-Partnern ein Vorschlag für ein „No-Spy-Abkommen“. Die Verhandlungsführerin auf US-Regierungsebene, die National Security Council Senior Director *Karen Donfried*, stellte rückblickend in einem

982) *Rheinische Post* vom 16. August 2013 „Interview mit dem Bundesinnenminister Friedrich: ‚Stolz auf unsere Geheimdienste‘„; Vorabmeldung *dpa* vom 15. August 2013, „Rheinische Post: Friedrich rechnet mit No-Spy-Abkommen noch vor der Wahl“.

983) E-Mail von *James Melville* an *Christoph Heusgen* (BKAmt) vom 15. August 2013, MAT A BK-1/7b, Bl. 497 f.

Schreiben des Weißen Hauses vom 8. Januar 2014 für den gesamten Gesprächszeitraum klar:

> „Dies wird kein No-Spy-Abkommen werden, und ich glaube, jeder hier auf unserer Seite hat das auch fortwährend die ganze Zeit über klar zum Ausdruck gebracht“.[984]

Noch deutlicher kann die Haltung der US-Seite in allen Gesprächen nicht zum Ausdruck gebracht werden, dass ein „No-Spy-Abkommen“ weder vorgeschlagen, noch zugesagt noch überhaupt Gesprächsthema war, wenn die diplomatische Höflichkeit noch halbwegs gewahrt wird.

Es ist lediglich über eine politische Erklärung zur Zusammenarbeit beider Nachrichtendienste und über ein Kooperationsabkommen gesprochen worden.

Solche Abkommen zur Zusammenarbeit der USA gab es mit den „Five Eyes“-Staaten. Aber auch mit diesen Ländern, die in Sicherheitsbereichen mit den USA traditionell so eng verbunden sind, wie kein anderes Land, gab und gibt es kein „No-Spy-Abkommen.“ Das bestätigte der Zeuge *Schindler* in seiner Befragung vor dem Ausschuss.[985] Auch dies spricht und sprach schon im August 2013 entscheidend dagegen, dass ausgerechnet Deutschland nun ein solches Abkommen angeboten wurde. Selbst mit Großbritannien, dem Staat, mit dem die USA die engste Kooperation im Geheimdienstbereich pflegt, haben die USA kein Abkommen, das die gegenseitige Überwachung vollständig ausschließt.

Der für Geheimdienstangelegenheiten zuständige Bundesminister *Pofalla* kann an ein solches völlig ungewöhnliches, ja einmaliges Angebot auch gar nicht geglaubt haben. Sonst hätte er dieses angebliche „Angebot“ für ein „No-Spy-Abkommen“ vielleicht im geheim tagenden PKGr mitgeteilt, aber keinesfalls am 12. August 2013 öffentlich verkündet und in eine weltweit verbreitete schriftliche Erklärung aufgenommen – und auch noch mit dem Zusatz ein solches „No-Spy-Abkommen“ sei stilbildend. Ihm als gewief-

984) Zitiert nach: *Süddeutsche Zeitung* vom 9. Mai 2015, „All the best“.

985) *Schindler*, Protokoll-Nr. 50 I, S. 122.

ter Berufspolitiker und Geheimdienstminister musste klar sein, dass in dem Augenblick, in dem er ein solches Angebot öffentlich macht und sogar noch als „stilbildend", also beispielhaft, für westliche Dienste bezeichnete, das Angebot tot war. Die USA mussten befürchten, dass daraufhin ihre anderen Partnerländer bis hin zu Russland und China, vorstellig werden, um auch in den Genuss eines solchen Abkommens zu kommen. Was sie Deutschland selbst angeboten und gewährt hatten, hätten sie anderen Staaten nicht verweigern können, ohne erheblichen diplomatischen Ärger zu riskieren. Aber mit Theorie und Praxis der US-Geheimdienste sowie ihrer Philosophie „we take all" wären solche „No-Spy-Abkommen" absolut unvereinbar und völlig ausgeschlossen gewesen. Gerade, dass der damalige Bundesinnenminister sowie der Kanzleramtschef so unbedarft öffentlich mit dem angeblichen „Angebot" umgingen, zeigt, dass beide selbst nicht an das Angebot und an eine Realisierbarkeit glaubten. Wenn sie es ernst gemeint hätten, wäre es auch unverantwortlich gewesen. Schon die öffentliche Verkündung des angeblichen Angebots hat offensichtlich dazu geführt, dass das Klima der Gespräche mit NSA-Direktor *Alexander* signifikant schlechter geworden ist, wie BND-Präsident *Schindler* nach seinem Gespräch vom November 2013 berichtete.

Es gab also nie ein „Angebot" für ein „No-Spy-Abkommen", sondern Verhandlungen zur Erarbeitung einer vertraulichen Vereinbarung der Geheimdienste NSA und BND für die konkrete Zusammenarbeit auf neuer Grundlage und für eine öffentliche gemeinsame politische Erklärung von USA und Deutschland, die diese Grundlagen abstrakt umschreiben sollte. Das wurde am 30. Oktober 2013 von den Abteilungsleitern *Heusgen* und *Heiß* aus dem Kanzleramt einerseits und der Beraterin des US-Präsidenten *Susan E. Rice* und US-Geheimdienstkoordinator *Clapper* besprochen und in einem Vermerk festgehalten.

Es ging der Bundesregierung nicht darum, mit Verhandlungsgeschick ein „No-Spy-Abkommen" zu erreichen, für das es kein *Angebot* – weder von US-Geheimdienstseite noch gar von der zuständigen Administration des Weißen Hauses gegeben hat, sondern Ziel der Erklärung vom 12. August 2013 war, mindestens bis zur Bundestagswahl das lästige und peinliche Thema „Ausspähen der NSA unter Freunden" vom Tisch zu bekommen.

Was schadet es da, dass ein „No-Spy-Abkommen" Deutschlands mit den USA bis heute nicht existiert und auch nicht in Sicht ist.

b) Keine Einhaltung von Recht und Gesetz in Deutschland

Die Beweisaufnahme hat ergeben, dass deutsches Recht und Gesetz entgegen allen Beteuerungen der NSA verletzt wurden.

1. In ihrer Erklärungsnot nach der Veröffentlichung der *Snowden*-Dokumenten versuchte die Bundesregierung und insbesondere die Bundeskanzlerin geradezu händeringend ab Mitte Juli 2013 von der US-Seite eine offizielle Bestätigung und Zusicherung zu erhalten, dass die US-Freunde tatsächlich deutsches Recht auf deutschem Boden beachten. Unter Berufung auf den Wunsch der Kanzlerin gab es einen intensiven Schriftverkehr zwischen dem Sicherheitsberater *Heusgen* im Kanzleramt, das die Achtung der deutschen Gesetze zur Schlüsselfrage der Beziehungen erklärte, und dem Weißem Haus, das diese Frage und die Interpretation der deutschen Gesetze zunächst prüfen wollte. Es wurden Textvorschläge für ein Abkommen getauscht. Bald stellte sich heraus, dass die US-Seite nicht daran dachte, deutsche Erwartungen, deutsche Bürger nicht auszuspähen, in Zukunft zu erfüllen und dies auch in der Vergangenheit nicht getan hatte.

2. Schon im Jahr 2005 verstieß die Übermittlung der Selektoren zu den Firmen „*EUROCOPTER*" und „*EADS*" durch die NSA zwecks Einsteuerung zum Ausspähen durch den BND gegen deutsches Recht. Im BND war dies 2005 aufgefallen. Der deutsche Nachrichtendienst hatte diese Selektoren deshalb damals aus der Erfassung herausgenommen. Der NSA wurde dies mitgeteilt und von ihr auch akzeptiert. Ihr war offensichtlich klar, dass der Einsatz dieser Suchbegriffe mit deutschem Recht nicht vereinbar war. Wirtschaftsspionage gehörte nicht zum Aufgabenbereich des BND und angeblich auch nicht der NSA, zumal dadurch eminent gegen deutsche Interessen vorstoßen wurde. Schließlich wurden damit zwei große deutsch-europäische Wirtschaftsunternehmen ausgespäht, die in einigen Produktbereichen in direkter Konkurrenz zu US-Firmen standen. Der BND war deshalb gewarnt und zu Recht skeptisch und misstrauisch gegenüber der NSA und teilte dies auch immer wieder dem Kanzleramt mit: Am 14. Februar 2008 warnte der

BND, „dass die US-Seite versucht, die Nachrichtengewinnung auf Bereiche auszudehnen, die nicht im deutschen Interesse sind." Im Juni 2010 schrieb der BND: „NSA hat jedoch in 2005 Erfassungskriterien zu den Firmen EADS, Eurocopter und verschiedenen französischen Behörden in JSA eingestellt. BND hat dies entdeckt und im Anschluss unterbunden." Zudem befürchtete der BND, „dass die NSA weiterhin gemäß US-Interessen deutsche Ziele aufklärt."[986]

3. Im BND war spätestens am Tag nach dem Auftritt *Pofallas* vom 12. August 2013 bereits bekannt, dass die NSA im Laufe der vorangegangenen Jahre tausende Selektoren, also Suchbegriffe, zugeliefert hatte, die gegen das MoA, also die US-deutsche Vereinbarung aus dem Jahr 2002 und gegen deutsches Recht verstoßen. Entsprechend bewerteten die zuständigen Fachleute des BND im August 2013 die Selektoren, die vom BND eingesteuert worden waren, und steuerten sie deshalb aus. Der Zeuge *D. B.*, Unterabteilungsleiter im BND, hatte Anfang August 2013 nach den Veröffentlichungen der Dokumente aus dem Besitz von Snowden und nach öffentlichen Erklärungen der Bundesregierung wie „Ausspähen unter Freunden geht gar nicht" Anlass gesehen, die von der NSA zur Verfügung gestellten und vom BND gesteuerten Selektoren insgesamt auf unzulässige und rechtswidrige zu überprüfen. Dabei waren sie auf die insgesamt 40.000 bemakelte NSA-Selektoren gestoßen und hatten diese aus der Steuerung genommen.

   Die ausgesonderten Selektoren betrafen u. a. Regierungsstellen von EU-Staaten, EU-Institutionen und Mitglieder befreundeter Regierungen, aber auch Deutsche. Sie waren nach Wertung der „Sachverständigen Vertrauensperson" der Bundesregierung, *Graulich*, nach dem MoA vertragswidrig. Sie gefährdeten potentiell die Beziehungen mit den EU-Partnern und schadeten deutschen Interessen erheblich. Ihr Einsatz war auch eine schwere Fehlleistung des BND. Im Falle des Bekanntwerdens dieser Ausspähpraktiken war nicht nur das Ansehen der Kanzlerin und der Bundesregierung sondern auch der BRD gefährdet. Wohl deshalb hat sich auch der spätere Kanzleramtschef *Altmaier* nach Bekanntwerden der Selektoren intern und öffentlich bestürzt und empört geäußert.

986) *Frontal21* vom 27. April 2015, „Nachgehakt – US-Wirtschaftsspionage: de Maiziere war ab Februar 2008 informiert".

Ob die Spitze des BND und das aufsichtführende Kanzleramt bereits im August 2013 vom Auffinden dieser bemakelten US-Selektoren Kenntnis erlangt hatten oder erst im März 2015, ist ungeklärt. Der Zeuge *D. B.* und andere BND-Mitarbeiter, die von dem Vorgang wussten, haben verneint, dass sie diese Information nach oben weitergegeben haben. Die Zeugen aus der Spitze des BND und aus dem Kanzleramt haben übereinstimmend betont, erst 2015 nach dem Beweisantrag der Opposition davon erfahren zu haben.

Aber fest steht, dass die zentrale Argumentation in der Erklärung *Pofallas* vom 12. August 2013, die NSA würden Gesetz und Recht in Deutschland einhalten, inhaltlich falsch war.

4. Die Vertreter von BND und Bundesregierung hatten genügend Anlass, an den immer wieder wiederholten Versicherungen der US-Verhandlungspartner aus den Geheimdiensten zu zweifeln, die NSA halte sich in Deutschland an Gesetz und Recht. Solche Zweifel waren geboten, weil die Chefs der US-Nachrichtendienste *Hayden* und *Alexander* immer wieder erklärten, die US-Dienste würden alle irgendwie verfügbaren Informationen abgreifen und nutzen. Das Programm lautete: „Let's collect the whole haystack (…) Collect it all, tag it, store it.“[987] Vor allem aber war der Presse und TV-Übertragungen zu entnehmen, dass der Director of National Intelligence *James Clapper* bei einer öffentlichen Befragung im US-Kongress am 12. März 2013 die Unwahrheit gesagt hatte. Auf die Frage des Senators *Ron Wyden*, ob die NSA in den USA Daten von Bürgerinnen und Bürger massenhaft ausgespäht hatten, antwortete er nach einigem Nachdenken mit: „No, Sir.“ Die Aussage war falsch. Später erklärte *Clapper* diese seine Aussage damit, wie die *Washington Post* am 12. Juni 2013 berichtete, er habe geantwortet, was er für das Glaubwürdigste hielt oder die am wenigsten unglaubwürdigste Weise, Nein zu sagen („I responded in what I thought was the most truthful, or least untruthful manner, by saying no.“).[988] *James Clapper* war der höchstrangige Vertreter der US-Geheimdienste und Gesprächspartner der Zeugen *Fritsche*, *Heiß* und *Schindler*.

987) *Washington Post* vom 14. Juli 2013, „For NSA chief, terrorist threat drives passion to 'collect it all'“.

988) *Washington Post* vom 12. Juni 2013, „James Clapper's 'least untruthful' statement to the Senate”.

Die *Washington Post* veröffentlichte dies am 12. Juni 2013 also nach den ersten Veröffentlichungen der Dokumente von *Snowden*, aber zwei Monate vor der Erklärung *Pofallas*. Danach durften die deutschen Gesprächspartner_innen nicht mehr davon ausgehen, dass die Beteuerungen der Vertreter_innen der US-Geheimdienste, diese würden sich in Deutschland an Gesetz und Recht halten, die pure Wahrheit sind. Wer einmal lügt, dem kann man nicht ohne weiteres glauben.

5. Das Ausspähen des Mobiltelefons der Bundekanzlerin ist ein Verstoß gegen deutsches Datenschutzrecht. Die geheimdienstliche Agententätigkeit durch eine fremde Macht ist strafbar.

   Die Beweisaufnahme hat ergeben, dass dieser strafbewehrte Gesetzesverstoß zumindest bis zum Telefonat der Bundeskanzlerin mit US-Präsident *Obama* Ende Oktober 2013 stattgefunden hat, denn sonst hätte der US-Präsident anders reagiert als mit der Versicherung, in Zukunft werde solches unterbleiben.

6. Im Juli 2014 war bekannt geworden, dass der BND-Mitarbeiter *Markus R.* seit Jahren – vermutlich schon seit 2008 – streng geheime Unterlagen – mindestens 218 Dokumente – hochbrisanten Inhalts wie etwa eine Liste aller BND-Agenten im Auslandseinsatz oder das Protokoll eines vom BND abgehörten Telefonats der damaligen US-Außenministerin *Hillary Clinton* gegen Zahlung von 75.000 Euro an den US-Geheimdienst verraten hatte. Wegen des Verrats im US-Auftrag durch diesen deutschen Mitarbeiter des deutschen Nachrichtendiensts kam es nach Pressemeldungen inzwischen zu einer Verurteilung zu einer Freiheitsstrafe von acht Jahren wegen des Verbrechens des Landesverrats. Der Fall macht mit größtmöglicher Deutlichkeit klar, dass US-Geheimdienste sich in Deutschland keineswegs an Gesetz und Recht halten. Die nachrichtendienstliche Agententätigkeit für eine fremde Macht verstößt gegen deutsches Recht und Strafgesetze. Misstrauen gegen gegenteilige Versicherungen der US-Seite war deshalb geboten und tut Not.

Hätte der Bundesminister im Kanzleramt *Pofalla* am 12. August 2013 nicht die falsche und unwahre Erklärung öffentlich verkündet, die US-Seite habe einen Vorschlag für ein „No-Spy-Angebot“ gemacht, wäre das Thema nicht vom Tisch gewesen. Die erst durch die Arbeit des Untersuchungsausschusses zu Tage getretenen Verstöße gegen

Recht und Gesetz hätten unmittelbar vor der Bundestagswahl die öffentliche Meinungsbildung und Debatte beeinflusst. In welchem Umfang Privatsphäre vor Eingriffen durch den Staat geschützt bleiben muss, hätten die Bürger_innen und Bürger unmittelbar durch ihre Stimmabgabe bestimmen können.

X. Das Versagen der Spionageabwehr im BfV

Wenn sich im Ergebnis des Untersuchungsausschusses diverse Verdachtsmomente auf Spionagetätigkeiten der Five-Eyes-Staaten vom Handy der Kanzlerin bis hin zu Wirtschaftsunternehmen wie *EADS* belegen lassen, stellt sich zwangsweise die Frage nach der Funktionsfähigkeit der Spionageabwehr. Laut Gesetz ist hierfür das Bundesamt für Verfassungsschutz (BfV) zuständig, in dem es

> „[…] Informationen, insbesondere von sach- und personenbezogenen Auskünften, Nachrichten und unterlagen, über […]
> 2. Sicherheitsgefährdende oder geheimdienstliche Tätigkeiten im Geltungsbereich dieses Gesetzes für eine fremde Macht […]“[989]

sammeln und auswerten soll.

Folgerichtig war die Rolle der Spionageabwehr auch Gegenstand des Untersuchungsauftrages, in dem u.a. folgende Fragen aufgeworfen wurden:

> „10. Welche Erkenntnisse über Art und Ausmaß derartiger Aktivitäten, die sich gegen in der Bundesrepublik Deutschland ansässige Wirtschaftsunternehmen richten, lagen Stellen des Bundes wann vor?
>
> 11. Hätten Stellen des Bundes gegebenenfalls schon zu einem früheren Zeitpunkt von derartigen Maßnahmen Kenntnis erlangen können beziehungsweise müssen? Gegebenenfalls welche Stellen wann?“[990]

1. Kein „360-Grad-Blick“

Nach dem Ende des Kalten Krieges wurde der Bereich Spionageabwehr innerhalb des BfV umstrukturiert, um sich an die neue Situation anzupassen. Neben diversen Referaten für einzelne Staaten gab es seit 1992 zusätzlich das sogenannte 360-Grad-Sachgebiet.[991] Dabei berichteten mehrere Zeugen übereinstimmend, dass der Spio-

989) § 3 Abs. 1 BVerfSchG.

990) Antrag auf Einsetzung eines Untersuchungsausschusses, Bundestagsdrucksache 18/843, S. 3.

991) Vgl. *Wingerath*, Protokoll-Nr. 98 I, S. 64 ff.

nageabwehr offenbar keine allzu große Bedeutung mehr beigemessen wurde. Der Referatsgruppenleiter im Bereich Grundsatz, Proliferation und Spionageabwehr im BfV *Frank Wingerath* dazu:

> „Sie müssen bitte sehen, dass die Ressourcen der Spionageabwehr begrenzt sind, stark begrenzt sind. Sie wurden noch stärker begrenzt nach dem Fall der Mauer, nachdem die DDR weggefallen ist als sicherlich wichtiges Land der Spionageabwehr. Die Ressourcen der Spionageabwehr wurden deutlich, deutlich gesenkt, immer weiter. Und dann nach 2001 – muss man dann auch bitte sehen –, nach 9/11 bestand nicht unbedingt das allgemeine politische Bedürfnis, ausgerechnet die Amerikaner, ohne dass es einen neuen Anlass oder Ähnliches gegeben hätte, intensiver zu bearbeiten als vorher.“[992]

Der Leiter der Abteilung 4 im BfV Spionageabwehr, Proliferationsabwehr, Wirtschaftsschutz sowie Geheim- und Sabotageschutz, *Dr. Burkhard Even*, betonte bereits im Eingangsstatement zu seiner Vernehmung vor dem Ausschuss die knappen Ressourcen aufgrund der Priorisierung innerhalb des Verfassungsschutzes:

> „Blick zurück in die 90erJahre: Nach dem Fall der Mauer und dem Ende des sogenannten Kalten Krieges wurde vielfach und nicht nur in Deutschland davon ausgegangen, dass das Thema Spionage erheblich an Bedeutung verloren habe. Infolgedessen gab es schon damals politische Entscheidungen, die Spionageabwehr deutlich zu reduzieren, was auch geschah. Nach den Ereignissen von 9/11 war es angesichts der enormen Bedrohungen durch den islamistischen Terrorismus, trotz dafür neu bewilligter Haushaltsstellen unumgänglich, weitere Stellen durch Umpriorisierung für diese Aufgabe zur Verfügung zu stellen. Deshalb wurden unter anderem im Bereich Spionageabwehr weitere personelle Ressourcen abgezogen.“[993]

---

992) *Wingerath*, Protokoll-Nr. 98 I, S. 85.

993) *Even*, Protokoll-Nr. 100 I, S. 6.

Gleichwohl machten die Vernehmungen deutlich, dass es neben dem scheinbar engen Personalkorsett weitere Gründe für die Beobachtung oder eben auch „Nicht-Beobachtung“ bestimmter Staaten gab. Vorherrschend sind nach wie vor die Freund-Feind-Schemata des Kalten Krieges, wie sich an einer Reihe von Aussagen diverser Zeugen nachvollziehen lässt.

> „Eine systematische Beobachtung, die immer auch sehr ressourcenintensiv ist, findet bei Bündnispartnern grundsätzlich nicht statt. Bei besonders wichtigen Bündnispartnern spielt zudem der Aspekt der engen Zusammenarbeit eine besondere Rolle. Gerade die USA sind ein ganz wichtiger Kooperationspartner, mit dem wir in vielen Bereichen – im Übrigen auch im Bereich Spionageabwehr – sehr eng und sehr vertrauensvoll zusammenarbeiten. Es ist aus meiner Sicht viel sinnvoller, die vorhandenen knappen Ressourcen für die Kooperation mit Partnern als für deren systematische Beobachtung einzusetzen.“[994]

Der Zeuge *Hans Josef Vorbeck* betonte in seiner Aussage, dass auch im Bereich Wirtschaftsspionage die Feindbilder klar verteilt sind:

> „Soweit ich mich erinnere, waren es die chinesischen und die russischen Dienste, denen man da große Fähigkeiten zuschrieb. Ich glaube, das ist heute nicht viel anders.“[995]

Ähnlich äußert sich in diesem Zusammenhang auch *Frank Wingerath* und bestätigte, dass die Five-Eyes-Staaten nicht mit auf der Liste der permanent zu beobachtenden Staaten standen.[996]

Für ausgewählte Staaten – China oder Russland wurden mehrfach genannt[997] – gibt es, vermutlich bis heute, eigene Referate innerhalb der Spionageabwehr des BfV, für alle übrigen Staaten (im Untersuchungszeitraum 155) gibt es das 360-Grad-Referat.

994) *Even*, Protokoll-Nr. 100 I, S. 6.

995) *Vorbeck*, Protokoll-Nr. 52 I, S. 106.

996) Vgl. *Wingerath,* Protokoll-Nr. 98 I, S. 65.

997) *Fritsche,* Protokoll-Nr. 57 I, S. 21; *Dr. Thomas de Maizière*, Protkoll-Nr. 55 I, S. 98

Es wird erst tätig, wenn es einen konkreten Verdacht bzw. Anlass gibt. Verdichten sich die Hinweise, erfolgt temporär eine systematische Bearbeitung dieses Landes. Wenngleich angegeben wurde, dass es für den Untersuchungszeitraum innerhalb der Spionageabwehr keine Anlässe zu einer anlassbezogenen Untersuchung von SIGINT Spionage durch die Five-Eyes-Staaten gab[998], so schloss zumindest der Zeuge *Frank Wingerath* nicht aus, dass es politische oder Wirtschaftsspionage durch die Five-Eyes-Staaten in Deutschland gab oder auch gibt:

> „Ich kann es auf gar keinen Fall ausschließen. Ich kann nur sagen: Ich hoffe nicht. Wir haben immer wieder Fälle oder Hinweise, dass so etwas vielleicht passiert, was den Untersuchungsgegenstand, die technische Spionage, betrifft, auch da aber in deutlich geringerem Prozentsatz.“[999]

Im Endeffekt scheint es sich beim 360-Grad-Referat eher um ein Placebo handeln. Die gesetzlichen Aufgaben gemäß §3 Abs. 1 Nr. 2 BVerSchG werden zwar theoretisch gewahrt, tatsächliche Spionageabwehr findet aber woanders statt.

Das *BfV* ist an dieser Stelle Opfer seines eigenen Freund-Feind-Schemas geworden. Beobachtet man bestimmte Staaten systematisch aus dem Blickwinkel der Spionageabwehr, so wird man viel eher zu Treffern gelangen, als wenn man auf einen konkreten Anlass wartet, welcher eine Bearbeitung rechtfertigt. Staaten im Pool des 360-Grad-Referates haben von der deutschen Spionageabwehr nicht viel zu befürchten. .

> „Wenn man nicht hinguckt, sieht man nur ganz, ganz selten was, und wenn man systematisch hinguckt, dann ist die Wahrscheinlichkeit sehr groß bei vielen Staaten, dass man was sieht. […] Aber es ist klar: Wenn ich beschränkte Ressourcen einsetze, dann finden bestimmte Dinge nicht statt. Und wenn ich mehr Ressource einsetze, dann kann

998) Vgl. *Wingerath,* Protokoll-Nr. 98 I, S. 64.

999) *Wingerath*, Protokoll-Nr. 98 I, S. 91.

> man deutlich mehr machen und erzielt dann auch entsprechende Erfolge, mit großer Wahrscheinlichkeit jedenfalls.“[1000]

Zum Ende der öffentlichen Befragung gesteht der Zeuge *Dr. Burkhard Even* ein

> „[…] aktuell sind die Five Eyes mit Sicherheit ein lohnendes Objekt der Bearbeitung, ja. […] Ich glaube die Nazis sind heute nicht mehr der Grund, warum amerikanische Dienste auch bei Deutschland hingucken.“[1001]

Im Untersuchungsausschuss konnten die angehörten Zeugen nicht schlüssig erläutern, warum bestimmte Staaten systematisch enger beobachtet werden als andere. Es gab in der jüngste Vergangenheit immer auch Hinweise auf Spionagetätigkeiten von US-Diensten. Dies hat die politischen Entscheidungsträger_innen nicht dazu bewogen, das Auftragsprofil der Bundesregierung entsprechend anzupassen. Innenminister *Dr. Thomas de Maizière* dazu:

> „Es ist nicht zu beanstanden, wenn Aktivitäten von Nachrichtendiensten befreundeter Staaten in Deutschland mit geringerer Intensität beobachtet werden als Aktivitäten gegnerischer Nachrichtendienste.“[1002]

2. Immer wieder Hinweise auf Spionageaktivitäten von US-Diensten

In Kapitel *V. Kooperation des BND mit der NSA: EIKONAL und Bad Aibling* wurde bereits ausführlich erörtert, mit welchen Methoden US-Dienste versuchten und vermutlich bis heute versuchen, Informationen über Ziele zu erhalten, die sich nicht aus den bekannten Zielen der Kooperation wie der Abwehr von Terrorismus, Waffenhandel oder Schutz des eigenen Militärs erklären lassen. EADS, Eurocopter und französischen Behörden gehören zu den bekanntgewordenen Zielen der NSA-Selektoren.[1003]

1000) *Even*, Protokoll-Nr. 100 I, S. 60 f.

1001) *Even,* Protokoll-Nr. 100 I, S. 62.

1002) *de Maizière*, Protokoll-Nr. 55 I, S. 97.

1003) Vgl. hierzu Kapitel V.8 – Verstöße bei Verwendung von NSA-Selektoren.

Die Zusammenarbeit zwischen BfV und Bundesnachrichtendienst (BND) im Bereich der Spionageabwehr beschrieb der *Zeuge Frank Wingerath* auf Nachfrage als „punktuell“[1004] und betonte, dass sich der gesetzliche Auftrag auf die Abwehr der Spionage durch eine fremde Macht beziehe.

> „Schon allein daraus geht hervor, dass das, was der BND macht, nicht unser Untersuchungsauftrag sein kann.“[1005]

Doch auch ohne die konkrete Anlässe wäre Vorsicht geboten gewesen. Die Vorwürfe der (Wirtschafts-)Spionage durch US-Dienste sind keine neuen Erkenntnisse des NSA/BND-Untersuchungsausschusses. Hinweise dafür gab es bereits in der Vergangenheit. Geändert wurde offenbar wenig.

a) Hinweise auf Wirtschaftsspionage

Spätestens seit der Veröffentlichung des *Echelon-Berichts*[1006] des Europäischen Parlaments im Juli 2001 musste auch der Bundesregierung und ihren Nachrichtendiensten klar sein, dass die Five-Eyes-Staaten nicht nur auf der Suche nach Staatsfeinden und Terroristen sind. Unter anderem kam das Europäische Parlament zu folgenden Erkenntnissen:

– Es bestehen keine Zweifel daran, dass das Echelon-System zum Abhören privater und wirtschaftlicher Kommunikation dient.[1007]

– Das Europäische Parlament fand schon damals beunruhigend, dass die verantwortlichen Stellen in den Mitgliedsländern keine Ahnung von der Existenz des weltweiten Abhörsystems hatten.[1008]

1004) *Wingerath*, Protokoll-Nr. 98 I, S. 7.

1005) *Wingerath*, Protokoll-Nr. 98 I, S. 55.

1006) Vgl. *Echelon-Bericht,* MAT A BND-2/2g, auch: Europäisches Parlament, Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)), abrufbar unter http://www.europarl.europa.eu/sides/getDoc.do?type=REPORT&reference=A5-2001-0264&format=XML&language=DE

1007) Vgl. *Echelon-Bericht,* MAT A BND-2/2g, Bl. 176.

1008) Vgl. *Echelon-Bericht,* MAT A BND-2/2g, Bl. 176.

– Die Nachrichtendienste der USA klären nicht nur allgemeine wirtschaftliche Sachverhalte auf, sondern auch und gerade die Kommunikation bei Wirtschaftsunternehmen, wenn es um Auftragsvergaben geht.[1009]

Unter Spionage verstehen die Verfasser_innen „nichts anderes als den organisierten Diebstahl von Informationen“[1010]. Sie hielten fest:

> „Schon vor 50 Jahren galt das Interesse nicht nur Informationen aus den Bereichen Politik und Sicherheit, sondern ebenso aus der Wissenschaft und Wirtschaft.“[1011]

> „Seit 1990 hat die amerikanische Regierung zunehmend wirtschaftliche und nationale Interessen gleichgesetzt […] wirtschaftliche Sicherheit [ist] ein integraler Bestandteil nicht nur der nationalen Interessen sondern auch der nationalen Sicherheit.“[1012]

Im Bericht des Europäischen Parlaments wird einerseits ausführlich dargestellt, dass bereits 2001 genügend Hinweise dafür vorlagen, dass die USA mit Hilfe eines weltweiten Sattelitennetzes aktiv Wirtschaftsspionage betrieben. Eine der dafür notwendigen Abhörstationen befand sich in Bad Aibling und somit auf deutschem Boden.

Andererseits macht der Bericht auch deutlich, dass die Grenzen des Echelon-Systems darin lagen, dass es lediglich zum Abhören von Satellitenkommunikation geeignet war. In Regionen mit dichten Glasfasernetzen wie Europa, erfolgt die Kommunikation jedoch eher leitungsgebunden, als via Satellit.[1013] Spätestens an dieser Stelle hätten auch die deutschen Dienste gewarnt sein müssen. Es ist nur folgeloisch, dass sich Dienste die Wirtschaftsspionage betreiben wollen (was der *Echelon-Bericht* zweifelsfrei feststellt) sich auch weitere Wege, jenseits der Satellitenkommunikation suchen, um an Informationen zu gelangen.

1009) Vgl. *Echelon-Bericht,* MAT A BND-2/2g, Bl. 178.

1010) Vgl. *Echelon-Bericht,* MAT A BND-2/2g, Bl. 190.

1011) *Echelon-Bericht,* MAT A BND-2/2g, Bl. 231.

1012) *Echelon-Bericht,* MAT A BND/2-2g, Bl. 275.

1013) Vgl. *Echelon-Bericht,* MAT A BND-2/2g, Bl. 236.

Nach Kenntnis des Berichtes sind Zeugenaussagen wie die des Zeugen *Dr. Thomas Kurz*, Referatsleiter in der für die Aufsicht der Geheimdienste zuständigen Abteilung 6 des Kanzleramts, wenig nachvollziehbar:

> „Und wir sind davon ausgegangen, dass die Amerikaner das nicht tun. […] Es gab nie einen Anhaltspunkt, dass dem so sein könnte.“[1014]

Der Zeuge *Hans Josef Vorbeck,* ebenfalls Abt. 6 des Kanzleramts*,* bestätigte dies:

> „Aber da waren die Schwerpunkte relativ deutlich immer in Richtung Osten. Und auch diese Echelon-Diskussion hat zumindest in Bezug auf Wirtschaftsspionage da nicht allzu viel dran geändert, weil wir eben, wie auch heute noch, der Überzeugung sind, dass die Wirtschaftsspionage in diesem engeren Sinne, wie ich es gemeint habe, von den USA nicht betrieben wird.“[1015]

Dabei gab es durch den Echelon-Bericht mehr als deutliche Anhaltspunkte dafür.

Nahezu alle zu diesem Untersuchungsgegenstand gehörten Zeugen aus den Reihen der Bundesregierung bzw. der ihr nachgeordneten Behörden betonten, dass es sich aufgrund der Verfasstheit des politischen und wirtschaftlichen Systems der USA ausschließe, dass Wirtschaftsspionage betrieben werde. Nach Lesart der meisten Zeugen wäre eine Begründung

> „[…], dass die amerikanischen Dienste Probleme hätten, diese Informationen dann weiterzugeben an die Firmen. Man hätte sie nie einem Unternehmen geben können, sondern – – Wir haben immer das Beispiel gehabt: Autohersteller. Wenn man es Ford gegeben hätte, hätte man es auch General Motors geben müssen, und das wäre nie und nimmer geheim geblieben.“[1016]

Credo der Dienste ist offensichtlich: Es kann nicht sein, was nicht sein darf.

1014) *Kurz*, Protokoll-Nr. 52 I , S. 38.

1015) *Vorbeck*, Protokoll-Nr. 52 I, S. 115 f.

1016) *Vorbeck*, Protokoll-Nr. 52 I, S. 107.

Als Ausweg aus dem Dilemma soll die Einteilung inWirtschaftsspionage einerseits und Konkurrenz- bzw. Industriespionage andererseits dienen. Der ehemalige Präsident des *BfV Heinz Fromm* dazu auf dem 5. Frankfurter Sicherheitstag:

> „Unter Wirtschaftsspionage […] ist die staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben zu verstehen. […] Bei der Konkurrenzausspähung (-Spionage) hingegen handelt es sich um die Ausforschung, die ein (konkurrierendes) Unternehmen gegen ein anderes betreibt.“[1017]

Im Verlauf der Untersuchung wurde jedoch darauf hingewiesen, dass die Übergänge zumeist fließend sind, insbesondere wenn es große staatliche oder halbstaatliche Unternehmen gibt, was auch der Zeuge *Guido Müller* bestätigte:

> „Ich glaube, das ist in der Tat eine der Krux: Was ist Wirtschaftsspionage, Konkurrenzausspähung, und was ist – in Anführungszeichen – der Versuch, Proliferationsinformationen zu erlangen? In der Tat ist die Trennschärfe ausgesprochen kompliziert.“[1018]

Die schwammigen Definitionen können aber nicht davon abzulenken, dass es eindeutige Hinweise dafür gibt, dass die Five-Eyes-Staaten in Deutschland auch Wirtschaftsunternehmen ausspionieren.

Ganz egal wie offensichtlich: Die Haltung der Bundesregierung ist in jedem Fall, dass es keine Wirtschaftsspionage durch die USA in Deutschland gebe.

Dies war wohl auch das Motiv für die falsche Beantwortung einer Kleinen Anfrage der Fraktion *DIE LINKE. im April 2015.* Hier hatte sie erklärt, es lägen

---

1017) *Fromm*, MAT A BfV-13c, Bl. 18.

1018) *Müller*, Protokoll-Nr. 52 I, S. 55.

> „weiterhin keine Erkenntnisse zu angeblicher Wirtschaftsspionage durch NSA oder anderen US-Diensten in anderen Staaten vor.“[1019]

Keine zwei Wochen nach dieser Antwort auf die Kleine Anfrage veröffentlichte das Magazin *Der Spiegel, dass*

> „[s]pätestens im Jahr 2010 […] im Kanzleramt BND-Meldungen [einliefen], wonach die USA versucht hatten, die Rüstungskonzerne EADS und Eurocopter auszuspähen. Diese Versuche, so ein geheimes Papier, wurden vom BND im Jahr 2005 entdeckt und „im Anschluss unterbunden“. Die Regierung hat die Existenz dieses Papiers bestätigt.“[1020]

Einen weiteren Hinweis auf Wirtschaftsspionage lieferte beispielsweise die *Wirtschaftswoche* in einem Beitrag vom Oktober 2010. Darin heißt es, dass u.a. das Bundesamt für Sicherheit in der Informationstechnik (BSI) davor warne, das mobile Mailsystem von *Blackberry* zu verwenden. Die genutzten Server liegen im Ausland und können daher gut für Wirtschaftsspionage genutzt werden.[1021]

[Platzhalter 1 – zur Herabstufung]

> [redacted].[1022]

Im Untersuchungszeitraum gibt es immer wieder Belege dafür, dass US-Dienste aktiv Wirtschaftsspionage in Deutschland betreiben. Warum die Bundesregierung dies aktiv übersieht, bleibt ihr Geheimnis.

1019) Antwort der Bundesregierung auf die Kleine Anfrage „Konsequenzen nach Angriff auf weltweit größten Chipkartenhersteller duch die Geheimdienste NSA und GCHQ“, Bundestagsdrucksache 18/4637, S. 3.

1020) *Spiegel Online* vom 29. April 2015, „Regierung machte falsche Angaben zur NSA-Spionage“, http://www.spiegel.de/politik/deutschland/bnd-affaere-kanzleramt-soll-nsa-selektoren-offen-legen-a-1031092.html, abgerufen am: 1. Juni 2017.

1021) Vgl. MAT A BSI/1-6d_5, Bl. 35 ff.

1022) MAT A BfV-13d (Tgb-Nr. 195/15 – GEHEIM), Anl. 02, Bl. 109.

b) Hinweise auf Spionage gegen TK-Infrastruktur

Neben den Hinweisen zu Wirtschaftsspionage ergaben sich aus den vorgelegten Beweismaterialien Hinweise auf Spionagetätigkeiten durch die Nachrichtendienste der Five-Eyes-Staaten und die Kenntnis dessen deutscher Dienste. Aus den Unterlagen geht hervor, dass

[Platzhalter 2 – zur Herabstufung]

[redacted].[1023]

c) NetBotz

Nach Recherchen des Fernseh-Magazins *FAKT* informierte der *BND* das Bundeskanzleramt spätestens 2005 über Erkenntnisse, nach denen der amerikanische Hersteller für Überwachungskameras *Netbotz* sogenannte Backdoors für amerikanische Geheimdienste einbaute. Netbotz-Kameras sind in einer nicht unerheblichen Zahl von sicherheitssensiblen Bereichen wie beispielsweise den Serverräumen des Frankfurter Flughafens verbaut. Die mit diversen Sensoren ausgestatteten Kameras können über eine spezielle Schnittstelle Daten direkt an amerikanische Geheimdienste ausleiten, ohne dass die Betroffenen davon erfahren. Der für die Spionageabwehr zuständige Verfassungsschutz erfuhr nach den vorliegenden Berichten erst 2015 und auch nur

1023) MAT A BMI-7/1l (Tgb-Nr. 25/14 – GEHEIM), Anl. 03, Ordner 7, Bl. 71-74.

zufällig durch Ermittlungen der Bundesanwaltschaft von diesem Vorgang.[1024] Von einem ähnlichen Vorgang berichtete bereits im Dezember 2014 das Nachrichtenmagazin *Der Spiegel*[1025].

Angesichts der Veröffentlichungen von *FAKT* im September 2016 und mit Bezugnahme auf den erwähnten Artikel im *Spiegel* fasste der Untersuchungsausschuss einen Beweisbeschluss zur Beiziehung aller Akten und Dokumente zum beschriebenen Vorgang, welche dem Bundesministerium des Innern (BMI) vorliegen[1026]. Die Erfüllung des Beweisbeschlusses wurde durch das BMI wie folgt abgelehnt:

> ,[redacted][1027]

Der Vertreter des BMI im Ausschuss, *MR Torsten Akmann* erklärte die Verweigerung der Aktenlieferung damit, dass es sich nicht um eine anlassunabhängige Überwachung handle und somit nicht vom Untersuchungsauftrag gedeckt sei. Vielmehr könne man das Raumüberwachungssystem mit einer Wanze vergleichen. Die Oppositionsfraktionen widersprachen dieser Auffassung und verwies einerseits auf Abschnitt B. Ziffer II. des Untersuchungsauftrages, denn die Überwachung von Serverräumen diene möglicherweise der Vorbereitug solcher Ausspähung. Auf der anderen Seite

---

1024) Vgl. „BND findet Spionage-Zugang in Überwachungssystemen – und schweigt“, http://www.mdr.de/fakt/fakt-usa-geheim-dienst-spionage-100.html, Stand: 12. Mai 2017, 13:39.

und „BND findet Spionage-Zugang in Überwachungssystemen – und schweigt, Manuskript“, http://www.mdr.de/fakt/ueberwachung-104-downloadFile.pdf, Stand: 12. Mai 2017, 13:41.

1025) Vgl. „Fern bedient“, http://www.spiegel.de/spiegel/print/d-130630551.html, Stand: 12. Mai 2017, 13:44.

1026) Beweisbeschluss BMI-26.

1027) Schreiben des BMI an den 1. Untersuchungsausschuss vom 15. November 2016, MAT A BMI-26 (VS-NfD)

könne durchaus von anlassloser Überwachung gesprochen werden, weil die betroffenen Unternehmen, Universitäten oder sonstigen Einrichtungen von der Datenerhebung und –ausleitung keine Kenntnis gehabt hätten. [1028]

Auch in diesem Fall folgte die Mehrheit allerdings der Haltung der Bundesregierung und lehnte den Beweisbeschluss ab.

Die Bundesregierung hat durch ihre Weigerungshaltung die Chance verpasst, die Vorgänge aufzuklären. So erhärtet sich der in den Berichten aufgeworfene Verdacht, dass es im Kanzleramt kein Interesse gab, aus den Berichten des BND die nötigen Konsequenzen zu ziehen und das zuständige BfV zu informieren. Sollte eine formale Prüfung im Kanzleramt stattgefunden haben, fehlt es offenbar an den entscheidenden Stellen an Problembewusstsein. Für den Fall, dass BMI und BfV doch informiert wurden, liegt der Verdacht nahe, dort niemand tätig wurde – warum sonst wäre dem Ausschuss die Einsicht in die Akten verweigert worden. Mit den Stimmen der Mehrheit wurde selbst die Akteneinsicht über das sogenannte Obleute-Verfahren verhindert, das dazu dient zu überprüfen, ob bestimmte Akten dem Untersuchungsgegenstand unterfallen.[1029]

Die automatisierte Überwachung sicherheitssensibler Bereichen wie Serverräume durch fremde Nachrichtendienste ermöglicht diesen wesentliche Erkenntnisse: Wann ist Personal in den Serverräumen und wann sind diese gänzlich ungeschützt, wer hat Zutritt zu Räumen, wie sind die Zugänge gesichert, etc. Auch das Mitlesen eingegebener Passwörter u.a. ist denkbar.

Auch am letzten hier skizzierten Fall lässt sich die bereits weiter oben gefasste Feststellung noch einmal erhärten: Wurden der für die Spionageabwehr zuständigen Stelle bewusst Informationen vorenthalten, gab es an Spionageabwehr offenkundig kein Interesse. Für das Verhalten der Bundesregierung und ihrer „Schutztruppe“[1030], der Mehrheit im Ausschuss, gibt es zwei mögliche Erklärungen: Entweder sollte die öffentliche Untersuchung verhindert werden, oder es besteht gar kein Interesse an der Unterbindung von Spionage in Deutschland durch die Five Eyes.

1028) Beratungsprotokoll-Nr. 117, S. 6.

1029) Beratungsprotokoll-Nr. 119. S. 5.

1030) Vgl. Kapitel II – Einleitung.

XI. Die Hauptstelle für Befragungswesen (HBW)

Bis zum Sommer 2014 betrieb der BND unter anderem in Berlin eine Tarnbehörde unter der Legende „Hauptstelle für Befragungswesen“ (HBW), in der teilweise unter Beteiligung von britischen oder US-amerikanischen Nachrichtendienstlern Asylbewerber_innen und andere Einwanderer_innen in Deutschland ausgehorcht wurden. Die Befragungen fanden im Rahmen des Programms „Integriertes Befragungswesen“ statt, einer Kooperation zwischen deutschen, amerikanischen, britischen und französischen Geheimdiensten.[1031]

Ausschusszeuge *Dr. August Hanning*, BND-Präsident von 1998 bis 2005, bezeichnete das Befragungswesen als „Relikt aus der alten Besatzungszeit, letztlich aus dem Kalten Krieg“[1032]. Allerdings sei ihm zu Beginn seiner Amtszeit als Präsident auf Nachfrage erklärt worden:

> „da seien doch wichtige Erkenntnisse auch in Sachen Irak und Naher Osten usw. gewonnen worden, und deswegen sei das sehr wichtig, die weiter aufrechtzuerhalten.“[1033]

Der Untersuchungsauschuss konzentrierte sich in den Zeugenvernehmungen hauptsächlich auf die Kooperation der HBW mit dem US-amerikanischen Militärnachrichtendienst Defence Intelligence Agency (DIA), und die Beantwortung der Frage, inwiefern Befrager_innen der DIA an Befragungen der HBW teilnahmen oder diese sogar eigenständig durchführten.[1034]

Die Zeugin *A. K.*, von 2008 bis zur formellen Auflösung der HBW im Juni 2014 als Leiterin der Behörde tätig, sowie *U. P.*, Befrager und Befragerführer von 2001 bis zur Auflösung, gaben beide an, es hätten neben der DIA keine anderen US-Geheimdienste direkt an Befragungen teilgenommen.[1035] Jedoch konnte sich die CIA indirekt am Befragungswesen beteiligen:

1031) *Hanning*, Protokoll-Nr. 65 I, S. 91.

1032) *Hanning*, Protokoll-Nr. 65 I, S. 91.

1033) *Hanning*, Protokoll-Nr. 65 I, S. 91.

1034) Vgl. Untersuchungsauftrag, Einsetzungsantrag vom 18. März 2014, B. 15. I., Bundestagsdrucksache 18/843.

1035) *A. K.*, Protokoll-Nr. 64 I, S. 32; *U. P.*, Protokoll-Nr. 110 I, S. 74.

> „Die CIA war nicht unmittelbarer integrierter Partner. Die CIA tritt aber in der Intelligence Community als teilweise sehr kräftiger Partner auf. Und da sind teilweise Interessen aufgekommen. Und dann musste man eben reagieren und sagen: ‚Das findet statt', oder: ‚Findet nicht statt'."[1036]

Grundlage der Zusammenarbeit seien schriftliche Vereinbarungen gewesen. Die USA beteiligte sich laut A. K. an den Kosten der HBW.[1037]

Die Tätigkeit der HBW und deren enge Kooperation mit US-Diensten war in mehrfacher Hinsicht problematisch: Zum einen drängt sich der Verdacht auf, dass an die USA weitergeleitete beziehungsweise von US-Befrager_innen erhobene Daten zu militärischen Zwecken, zum Beispiel für tödliche Drohnenangriffe, verwendet werden konnten. Dieser Verdacht liegt nicht fern, bedenkt man die fatalen Folgen, welche die an US-Dienste weitergeleiteten (Fehl-)Angaben des von der HBW befragten Informanten „Curveball" im Jahr 2003 auslösten.[1038] Deshalb war die konkrete Gestaltung der Kooperation mit den US-Nachrichtendiensten von hohem Interesse für den Ausschuss.

Zum anderen ist unklar, inwiefern Befragungen mit Asylbewerber_innen Einfluss auf deren Asylverfahren hatte. Klar ist, dass HBW und das Bundesamt für Migration und Flüchtlinge (BAMF) eng miteinander zusammenarbeiteten, was sowohl durch die Aussage der Zeugin *A. K.* gestützt wird als auch durch die der leitenden BAMF-Angestellten *Renate Leistner-Rocca*.

1. Unzulässige Befragungspraxis

In einem Bericht des ARD-Fernsehmagazins Panorama im November 2013 berichtete ein aus Somalia nach Deutschland Geflüchteter von seiner Befragung durch die HBW.

1036) *A. K.*, Protokoll-Nr. 64 I, S. 67.

1037) *A. K.*, Protokoll-Nr. 64 I, S. 67.

1038) Frankfurter Allgemeine Zeitung vom 22. Februar 2008, „Waffe der Massendesinformation", http://www.faz.net/aktuell/feuilleton/politik/waffe-der-massendesinformation-1516823.html, abgerufen am 25. Mai 2017).

Er habe ihnen die Telefonnummer eines Anführers der Al-Shabaab-Miliz gegeben. Auf welche Art diese verwendet worden sei, wisse er nicht.[1039]

Dass solche Informationen, wenn sie an US-Dienste weitergegeben werden, als HUMINT – „Human Intelligence“ (menschliche Quellen) – zur Lokalisierung von Zielpersonen für Drohnenangriffe verwertet werden, ist nicht auszuschließen.[1040]

Im Fokus der Vernehmungen im Untersuchungsausschuss stand deshalb die genaue Befragungspraxis – die Auswahl der Befragten, der Inhalt der Befragungen, die Form der Beteiligung von AND-Mitarbeiter_innen sowie die Frage, ob auch alleinige Befragungen durch DIA-Mitarbeiter_innen stattgefunden hätten.

a) Brotpreise oder Militärdaten?

Die Angaben der ehemaligen HBW-Leiterin *A. K.* zu Inhalten der Befragungen fielen eher vage aus. Es sei um „Informationsgewinnung zu zentralen Fragen, […] Politik, Wirtschaft, […] Versorgungslage und Ähnliches mehr“[1041] gegangen.

So sei beispielsweise bezüglich der Versorgungslage nach Brotpreisen gefragt worden.[1042] Personenbezogene Daten wie E-Mail-Adressen oder Handynummern hätten nicht im Mittelpunkt der Befragungen gestanden.[1043] Frau *K.* war allerdings selbst nicht bei Befragungen dabei und meinte an anderer Stelle, sich daher nicht konkret zu Befragungsinhalten äußern zu können.[1044]

1039) *Panorama* Nr. 774 vom 28. November 2013, „Geheimer Krieg: Die verborgenen Operationen der US-Dienste in Deutschland”, Film: 00:22:26 min, http://www.ardmediathek.de/tv/Panorama/Panorama-Geheimer-Krieg/Das-Erste/Video?bcastId=310918&documentId=18359668 (abgerufen am 26. Mai 2017), Skriptum: S. 6, https://daserste.ndr.de/panorama/archiv/2013/panorama4781.pdf (abgerufen am 26. Mai 2017).

1040) Vgl. hierzu Kapitel XII.4.h) – Identifizierung von Zielpersonen für US-Drohnenangriffe durch Metadaten und „Skynet“

1041) *A. K.*, Protokoll-Nr. 64 I, S. 12.

1042) *A. K.*, Protokoll-Nr. 64 I, S. 12.

1043) *A. K.*, Protokoll-Nr. 64 I, S. 96 f.

1044) *A. K.*, Protokoll-Nr. 64 I, S. 105.

Der ehemalige Befrager und Befragerführer *R. C.* antwortete auf die Frage, ob sich die Befrager_innen auch für Kontaktdaten interessiert hätten oder ob tatsächlich nur Fragen zur allgemeinen Stimmung im Herkunftsland Inhalt der Befragungen gewesen seien:

> „Nein, es waren durchaus auch, ja, ich sage mal, Themen, für die sich typischerweise ein militärischer Dienst interessiert.“[1045]

In nicht-öffentlicher Sitzung führte der Zeuge aus, natürlich seien auch Telefonnummern und Personenangaben abgefragt worden.[1046]

R. C. gab ebenfalls an, es sei um die Identifizierung und Lokalisierung von Objekten gegangen.[1047] Dabei sei Kartenmaterial wie Google Earth, Google Maps und ähnliches verwendet worden, in denen die Befragten Markierungen vornehmen sollten.[1048] Aus der Befragung des früheren Drohnen-Co-Piloten *Brandon Bryant* ging hervor, dass zur Planung von Drohneneinsätzen auch Kartenmaterial mit Einzeichnungen verwendet werde.[1049]

Ex-HBW-Befrager *R. C.* meinte zwar, er habe keine Anhaltspunkte dafür, dass die dabei gewonnenen Daten vom US-Militär für Drohneneinsätze verwendet worden seien, könne dies aber auch nicht ausschließen.[1050]

Amos Guoira, früher selbst an der Koordinierung von tödlichen Drohnenangriffen beteiligt, erklärt in dem Panorama-Bericht, jede Information fließe in das Zielerfassungssystem ein.[1051]

1045) *R. C.*, Protokoll-Nr. 110 I, S. 22.

1046) *R. C.*, Protokoll-Nr. 110 II – Auszug offen, S. 4.

1047) *R. C.*, Protokoll-Nr. 110 I, S. 19.

1048) *R. C.*, Protokoll-Nr. 110 II – Auszug offen, S. 6 f.

1049) *Bryant*, Protokoll-Nr. 67 Teil 1, S. 155.

1050) *R. C.*, Protokoll-Nr. 110 I, S. 19; vgl. dazu Kapitel XII Geheimer Krieg – Die Beteiligung Deutschlands am US-Drohnenkrieg.

1051) *Panorama* Nr. 774 vom 28. November 2013, „Geheimer Krieg: Die verborgenen Operationen der US-Dienste in Deutschland”, Film: 00:23:44 min, http://www.ardmediathek.de/tv/Panorama/Panorama-Geheimer-Krieg/Das-Erste/Video?bcastId=310918&documentId=18359668 (abgerufen am 26. Mai 2017), Skriptum: S. 7, https://daserste.ndr.de/panorama/archiv/2013/panorama4781.pdf (abgerufen am 26. Mai 2017).

b) Befragungen mit „gestandenen Praktikanten"

Die Zeugin *A. K.* gab an, zu ihrer Zeit habe die HBW in vier Außenstellen gearbeitet, die zum Ende des Untersuchungszeitraums immer weiter reduziert worden seien.[1052]

Insgesamt seien von 100 Mitarbeiter_innen 50 als Befrager_innen beschäftigt gewesen, die jährlich etwa 300 Befragungen durchgeführt hätten.[1053] Der Zeuge *R. C.* erklärte, gegen Ende der HBW seien es eher 15 Befrager_innen gewesen, die Zahl der Befragungen pro Jahr schätzte er auf 400 bis 500.[1054]

Bis zu zehn DIA-Mitarbeiter_innen seien bei der Behörde beschäftigt gewesen.[1055]

Sie als HBW-Leiterin habe das Weisungsrecht über die US-Befrager_innen gehabt, so Frau *K.*:

> „Wenn ich entschieden habe: ‚Da geht dieser Mensch nicht mit, zur Befragung', ist er nicht mitgegangen. Wenn ich gesagt habe: ‚Der geht mit', ging der mit."[1056]

Die DIA habe überwiegend „im Team mit Deutschen oder BND"[1057] befragt, aber das sei aus personeller Hinsicht nicht hunderprozentig umsetzbar gewesen. Es sei dehalb auch vorgekommen, dass US-Befrager_innen Befragungen allein durchgeführt hätten.[1058]

Aus einer BND-Akte ging hervor, auch die gemischten Teams hätten nicht immer aus HBW-Befrager_innen und dem US-Pendant bestanden.[1059] Auf Nachfrage führte Frau *K.* dazu aus, aufgrund des zunehmenden Personalmangels der HBW hätten auch andere Mitarbeiter_innen Befragungen zusammen mit der DIA durchgeführt:

1052) *A. K.*, Protokoll-Nr. 64 I, S. 12; zu Außenstellen der HBW vgl. auch Abschlussbericht, Zweiter Teil: Feststellungen des Untersuchungsausschusses, S. 143.

1053) *A. K.*, Protokoll-Nr. 64 I, S. 13.

1054) *R. C.*, Protokoll-Nr. 110 I, S. 61

1055) *A. K.*, Protokoll-Nr. 64 I, S. 14.

1056) *A. K.*, Protokoll-Nr. 64 I, S. 74.

1057) *A. K.*, Protokoll-Nr. 64 I, S. 14.

1058) *A. K.*, Protokoll-Nr. 64 I, S. 14.

1059) MAT A BND-2/3c, Ordner 375, Bl. 43 ff. (VS-NfD)

> „Das waren dann eben diese langjährigen Bürosachbearbeiter oder ein gestandener Praktikant.“[1060]

Das ist insofern bemerkenswert, als in einer Hintergrundinformation des BND anlässlich einer Aktuellen Frage im Bundestag zur HBW im November 2013 zur Arbeitsweise der HBW explizit erklärt wird:

> „[redacted]“[1061]

c) Teilnahme von AND-Mitarbeiter_innen an HBW-Befragungen ohne Rechtsgrundlage

Die Einbindung ausländischer Nachrichtendienste (AND) in die Informationserhebung, insbesondere der US- und der britischen Geheimdienste in die Befragungen durch die HBW erfolgte, ohne dass sich eine entsprechende Rechtsgrundlage findet. Weder das Gesetz über den Bundesnachrichtendienst (BNDG) noch die Einrichtung des integrierten Befragungswesens durch das Bundeskanzleramt boten eine ausreichende Grundlage für diese Praxis. Einer solcher bedurfte es jedoch, weil es sich bei der Befragung um einen rechtfertigungsbedürftigen Grundrechtseingriff handelte.

Denn die Befragungen der HBW unter Teilnahme oder sogar lediglich von AND-Mitarbeiter_innen griffen in den Schutzbereich des Rechts auf informationelle Selbstbestimmung der Befragten ein. Dies gewährleistet die Befugnis „grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“[1062]. Grundrechtsträger_innen sollen wissen können, „wer was wann und bei welcher Gelegenheit über sie weiß“[1063]. Dieses Gebot dürfte hier schon mangels Transparenz über den Zweck der Befragung, die Identität der Behörde und die Bedeutung ihrer Aussagen im Hinblick auf mögliche Konsequenzen verletzt sein. Von einer „freien Entscheidung“ im Sinne einer Einwilligung nach § 4a Abs. 1 Bundesdatenschutzgesetz

---

1060) *A. K.*, Protokoll-Nr. 64 I, S. 37.

1061) BND: Hintergrundinformation zur Unterrichtung der Bundesregierung über das Befragungswesen des Bundesnachrichtendienstes vom 26. November 2013, MAT A BND-2/2a, Bl. 352-355 (354) (VS-NfD).

1062) BVerfGE 65, 1 (43) (Volkszählungsurteil), https://openjur.de/u/268440.html.

1063) BVerfGE 65, 1 (43) (Volkszählungsurteil), https://openjur.de/u/268440.html.

(BDSG) kann schon deswegen nicht die Rede sein. Die Befragung ist und bleibt eine im weitesten Sinne verdeckte Maßnahme, die einer bereichsspezifischen Rechtsgrundlage bedarf, die ihrerseits die Beteiligung ausländischer Geheimdienste als Intensivierung des Grundrechtseingriffs abdeckt.

aa) Keine Rechtsgrundlage im BNDG

Eine solche erforderliche Rechtsgrundlage liegt aber insbesondere nicht in § 2 BNDG, der explizit den BND zur Informationsgewinnung ermächtigt und hierbei gerade nicht die Inanspruchnahme von Dritten umfasst. Auch § 3 BNDG stellt hierfür keine geeignete Rechtsgrundlage dar, insofern dieser sich mit der heimlichen Beschaffung von Informationen befasst und es sich bei der Befragung selbst ja gerade nicht um eine solche heimliche Maßnahme handelt, auch wenn es sich bei der HBW um eine Legendenbehörde handelt.

Selbst wenn man § 3 BNDG als rechtliche Grundlage der Arbeit der HBW unter Legende betrachtet, so bietet die Norm noch keine Rechtsgrundlage für die Beteiligung der AND.

Dies ergibt sich bereits aus dem Wortlaut der Norm in der Zeit des Untersuchungszeitraums. Dieser lautete:

> „Der Bundesnachrichtendienst darf zur heimlichen Beschaffung von Informationen einschließlich personenbezogener Daten die Mittel gemäß § 8 Abs. 2 des Bundesverfassungsschutzgesetzes anwenden, wenn Tatsachen die Annahme rechtfertigen, dass dies zur Erfüllung seiner Aufgaben erforderlich ist. § 9 des Bundesverfassungsschutzgesetzes ist entsprechend anzuwenden."

§ 8 Abs. 2 Satz 1 des Bundesverfassungsschutzgesetzes (BVerfSchG) lautete:

> „Das Bundesamt für Verfassungsschutz darf Methoden, Gegenstände und Instrumente zur heimlichen Informationsbeschaffung, wie den Einsatz von Vertrauensleuten und Gewährspersonen, Observationen, Bild- und Tonaufzeichnungen, Tarnpapiere und Tarnkennzeichen anwenden."

Die Mitarbeiter der AND waren jedoch gerade keine „Instrumente zur heimlichen Informationsbeschaffung“ und insbesondere keine Vertrauensleute oder Gewährspersonen.

bb) Keine Rechtsgrundlage durch hypothetischen Ersatzeingriff wegen Verstoß gegen Datenübermittlungsvorschriften

Auf eine parlamentarische Anfrage des Abgeordneten *Jan Korte* (DIE LINKE.) am 28. November 2013 zur fragwürdigen Befragungspraxis der HBW mit AND versicherte die Bundesregierung:

> „Die Befragungsergebnisse der alliierten Befrager werden im Meldungssystem des BND erfasst und dort einer Freigabeprüfung unterzogen. Erst nach der Freigabe erfolgt die Übermittlung nach § 9 Abs. 2 BND-Gesetz an den alliierten Partnerdienst.
>
> Die an die Partner weiterzugebenden Meldungen werden bei Bedarf bereinigt (im Hinblick auf Datenschutzgründe, Nichtweitergabe möglicher militärisch nutzbarer Daten). Es gelangen circa 60 Prozent der im Befragungswesen erhobenen Meldungen im Weitergabeverbund an die Partnerdienste.“[1064]

Laut einer BND-Akte wurde das für die HBW zuständige BND-Referat jedoch erst am 15. November 2013 in einer E-Mail [redacted].[1065]

Die Zusicherung der Bundesregierung bezüglich der Nichtweitergabe möglicher militärisch nutzbarer Daten kam also knappe zwei Wochen nach genannter BND-E-Mail mit der entsprechenden Weisung. Es muss also davon ausgegangen werden, dass eine solche Bereinigung vorher nicht oder zumindest nicht in jedem Fall stattgefunden hat.

1064) Antwort des Staatssekretärs *Dr. Schröder* auf die Mündliche Frage des MdB *Jan Korte* (DIE LINKE.) vom 28. November 2013, Plenarprotokoll 18/3, S. 212 f.

1065) E-Mail des BND-Referats EAZA an das BND-Referat EAC, MAT A BND-2/5c, Bl. 129 (VS-NfD).

Selbst wenn vom BND an AND weitergegebene Daten ab einem gewissen Zeitpunkt bereinigt wurden, so war die Kontrolle der Informationsweitergabe bei Anwesenheit von AND-Befrager_innen unmöglich – erst recht bei von ihnen allein durchgeführten Befragungen.

Deshalb ist davon auszugehen, dass durch Befragungen mit oder durch AND-Mitarbeiter_innen gleichzeitig auch Daten übermittelt worden sind.

Die Datenübermittlung erfolgte aber rechtswidrig und konnte nicht als Rechtsgrundlage für die gemeinsame oder alleinige Datenerhebung durch die AND-Mitarbeiter_innen im Sinne einer hypothetischen Ersatzvornahme dienen.

Nach der Rechtsprechung wird von der Zulässigkeit der Datenweitergabe ausgegangen, wenn die Empfänger_innen die Daten zu dem Zweck, zu dem sie sie erhalten, und unter den Umständen, unter denen sie erhoben wurden, auch selbst hätten erheben dürfen. Hieraus ließe sich im Umkehrschluss argumentieren, dass es bei einer Befragung, bei der die gesetzlichen Voraussetzungen für eine Weitergabe der Daten an den AND vorlagen – in diesem Fall § 9 Abs. 2 BNDG i.V.m. § 19 Abs. 3 BVerfSchG – nicht darauf ankäme, ob die Daten erst durch den BND erfasst und dann an den jeweiligen AND übermittelt oder gleich gemeinsam erhoben wurden.

Nach den Angaben von BND und Bundesregierung sei diese Weitergabe von Daten und Erkenntnissen der HBW auf der Grundlage des § 9 BNDG i.V.m. § 19 Abs. 3 BVerfSchG erfolgt.[1066]

§ 19 Abs. 3 BVerfSchG lautet:

> „Das Bundesamt für Verfassungsschutz darf personenbezogene Daten an ausländische öffentliche Stellen sowie an über- und zwischenstaatliche Stellen übermitteln, wenn die Übermittlung zur Erfüllung seiner Aufgaben oder zur Wahrung erheblicher Sicherheitsinteressen des Empfängers erforderlich ist. Die Übermittlung unterbleibt, wenn

1066) Hintergrundinformation zur Unterrichtung der Bundesregierung über das Befragungswesen des Bundesnachrichtendienstes MAT A BK-2/8f, Bl. 23 (VS-NfD); Antwort der Bundesregierung auf eine Kleine Anfrage der Fraktion DIE LINKE. vom 19. Dezember 2013, Bundestagsdrucksache 18/215, S. 5.

> auswärtige Belange der Bundesrepublik Deutschland oder überwiegende schutzwürdige Interessen des Betroffenen entgegenstehen. Die Übermittlung ist aktenkundig zu machen. Der Empfänger ist darauf hinzuweisen, dass die übermittelten Daten nur zu dem Zweck verwendet werden dürfen, zu dem sie ihm übermittelt wurden, und das Bundesamt für Verfassungsschutz sich vorbehält, um Auskunft über die vorgenommene Verwendung der Daten zu bitten."

Eine Übermittlung setzt damit eine umfassende Prüfungspflicht des BND über den Inhalt, die Bedeutung und die Verwendung der Informationen voraus.

In der Wertung der Koalition wurde dabei „im Einklang mit den gesetzlichen Vorgaben – jeweils im Einzelfall geprüft, ob schutzwürdige Interessen des Betroffenen das Allgemeininteresse an der Übermittlung überwogen. Die Übermittlung erfolgte immer unter der Bedingung, dass die Informationen nicht für unangemessenen Maßnahmen verwendet werden durften (z.B. Folter, Verurteilung zum Tod)." Zudem seien die weiterzugebenden Meldungen im Hinblick auf den Datenschutz und mögliche militärisch nutzbare Daten bereinigt worden. Die Beweisaufnahme habe keinen Hinweis darauf erbracht, dass Inhalte der Befragungen dem BND vorenthalten oder an diesem vorbei direkt an die jeweiligen ausländischen Nachrichtendienste übermittelt worden wären.[1067]

Eine solche Bewertung allerdings verweigert sich dem Gesetz der Physik, welches lautet, dass man nicht gleichzeitig an einem Ort anwesend und nicht anwesend sein kann. Waren die Mitarbeiter_innen der AND bei einer Befragung anwesend oder haben diese sogar gänzlich ohne Beteiligung der BND-Mitarbeiter_innen geführt, so konnte naturgemäß eine solche Einzelfallprüfung oder Informationsbereinigung gerade nicht stattfinden, da die Übermittlung zeitlich mit der Erhebung der Daten zusammenfiel. Nach den Aussagen der HBW-Leiterin *K.* konnte sie zudem nur darüber entscheiden, wer die Befragungen durchführt, nicht, welche der erhobenen Informationen

1067) Bewertung des Ausschusses durch die Mehrheit, Fassung vom 28. April 2017, S. 126 (VERWEIS AUF AKTUELLE SEITENZAHL)

zur Weitergabe qualifiziert sind und unter welchen Voraussetzungen.[1068] Diese Auswahl habe die Stelle „Auftragssteuerung und Koordinierung“[1069] getroffen:

> „[…] der Auswerter hat darüber entschieden, ob eine Meldung an den AND weitergegeben werden darf oder nicht.“[1070]

Weil aber bereits die gemeinsame Informationserhebung nicht aufgrund einer Rechtsgrundlage erfolgt ist, hätte es einer solchen Einzelfallprüfung i.S.d. § 9 Abs. 2 BNDG i.V.m. § 19 Abs. 3 BVerfSchG bedurft. Weder eine Erforderlichkeitsprüfung, noch eine Abwägungsentscheidung im Einzelfall vor dem Hintergrund schützwürdiger Interessen des oder der Betroffenen oder einem Hinweis auf die Zweckbindungsmaßgabe konnte überhaupt durch die Mitarbeiter_innen des BND in den Fällen getroffen werden, in denen Mitarbeiter_innen des AND bei den Befragungen anwesend waren, da die Informationen ja gleichzeitig mit ihrer Erhebung an die Mitarbeiter_innen der AND übermittelt wurden. Mehr noch – in den Fällen solcher Befragungen, an denen BND-Mitarbeiter_innen überhaupt nicht anwesend waren, konnte eine Prüfung, die zu einer Datenübermittlung „im Einklang mit den gesetzlichen Vorgaben“ notwendig gewesen wäre, gar nicht stattfinden. Der BND hatte in diesen Fällen keinerlei Hoheit über die Art von Daten, die erhoben und gleichzeitig übermittelt wurden. Die Datenübermittlung erfolgte im Widerspruch zu den Datenübermittlungsvorschriften des BNDG.

cc) Errichtung aufgrund eines öffentlichen Organisationsaktes der Bundesregierung keine taugliche Rechtsgrundlage

Die Tatsache, dass die HBW als Legendenbehörde für das integrierte Befragungswesen „[redacted][1071] wurde, stellt ebenfalls keine taugliche Rechtsgrundlage für die Einbindung ausländischer Nachrichtendienste in die Informationsgewinnung des BND dar. Insbesondere war die HBW nicht als

1068) *A. K.* Protokoll-Nr. 64 I, S. 9 f.

1069) *A. K.* Protokoll-Nr. 64 I, S. 64.

1070) *A. K.* Protokoll-Nr. 64 I, S. 64.

1071) Hintergrundinformation des Bundesnachrichtendienstes über das Befragungswesen vom 25. November 2013, MAT A BK-2/8f, Bl. 22-25 (22) (VS-NfD).

Dienststelle von den Alliierten übernommen, sondern nach Verzicht der Alliierten auf ihre Kontrollrechte neu eingerichtet worden.[1072]

Im Organisationsakt der Bundesregierung wurde die HBW vielmehr als eine deutsche Einrichtung unter deutscher Leitung eingerichtet. Zudem wurde Folgendes festgelegt:

> „Die beteiligten Partner haben das Recht auf das Einbringen eigener Befrager, die jedoch folgenden Einschränkungen unterliegen: Sie müssen nach außen hin als Deutsche auftreten, und sie unterstehen fachlich dem deutschen Dienststellenleiter."[1073]

Dieser Logik folgend berichtete auch die Zeugin *A. K.*, Leiterin der HBW von 2008-2014, die Mitarbeiter_innen der AND seien „quasi Erfüllungsgehilfen von uns"[1074] gewesen.

Selbst wenn man der Aussage der Zeugin Glauben schenken möchte (trotz des fragwürdigen Ober-Unterordnungsverhältnisses, auf welches sich die AND hierfür eingelassen haben müssen), so bildet weder die Tatsache, dass das Kanzleramt 1958 mittels einen unveröffentlichten Organisationsaktes die HBW als Legendenbehörde eingerichtet hat, noch die Tatsache, dass sich die AND-Mitarbeiter_innen als „Erfüllungsgehilfen" des BND gerierten, eine Rechtsgrundlage für die Befragung durch die Mitarbeiter der AND.

Dafür, eine solche Rechtsgrundlage zu schaffen, fehlte es dem Bundeskanzleramt im Übrigen auch an der Kompetenz. Denn die Gesetzgebungskompetenz für Befugnisse des BND liegt gemäß Art. 73 Abs. 1 Nr. 1 GG beim Bundesgesetzgeber, also beim Parlament, und nicht bei der Bundesregierung. Eine solche ergibt sich auch nicht aus der Fach- und Dienstaufsicht des Kanzleramts über den BND, die nur die Ausführung des Gesetzes betrifft.

1072) Vgl. Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion PDS/Linke Liste vom 29. Juli 1991, Bundestagsdrucksache 12/996, S 1.

1073) Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion PDS/Linke Liste vom 29. Juli 1991, Bundestagsdrucksache 12/996.

1074) *A. K.* Protokoll 64 I, S. 74.

Auch wenn die Frage offen bleibt, ob die Bundesregierung im Rahmen der Fach- und Dienstaufsicht des Kanzleramts über den BND die HBW als Legendenbehörde errichten durfte[1075] – jedenfalls konnte sie aber keine Rechtsgrundlage für die Beteiligung der US- und britischen Dienste an den Befragungen der HBW schaffen.

Die Praxis der Teilnahme von US- und britischen Diensten an Befragungen der HBW erfolgte folglich ohne Rechtsgrundlage und erfolgte somit unzulässigerweise.

d) Durchführung von Befragungen zur Informationserhebung ohne Teilnahme des BND rechtswidrig

Bereits die Beteiligung der Mitarbeiter_innen der AND erfolgte, wie dargelegt, ohne Rechtsgrundlage und war damit unzulässig. Die Durchführung von Befragungen *ohne* Teilnahme des BND war dann aber erst recht unzulässig. An einer Rechtsgrundlage für eine alleinige Informationserhebung durch die AND fehlt es.

Eine solche Rechtsgrundlage ergibt sich insbesondere auch nicht durch die von der Zeugin A. K. erwähnten[1076] vertraglichen Vereinbarung zwischen dem BND und den AND, welche die Details der Zusammenarbeit im Rahmen der HBW regelten. Wie bereits dargelegt konnte weder die Bundesregierung, geschweige denn der BND selbst die Rechtsgrundlagen zur Erhebung von Informationen schaffen, sondern wären hierfür auf einen Rechtssetzungsakt des Bundesgesetzgebers angewiesen gewesen.

Dass es rechtlich unzulässig ist, dass ausländische Dienste alleinige Befragungen durchführen, müsste den BND-Mitarbeiter_innen auch bewusst gewesen sein. Zumindest wird es in deren Ausbildung gelehrt. Folgendes findet sich in einem Skript zum „Recht der Nachrichtendienste“, das als Schulungsmaterial für zukünftige deutsche Geheimdienstmitarbeiter_innen dient:

1075) Art. 87 Abs. 3 Satz 1 GG spricht von der Einrichtung selbstständiger Bundesoberbehörden *durch* Bundesgesetz, womit sich die Frage stellt, inwieweit sich die Binnendifferenzierung selbst aus dem Gesetz ergeben muss oder auf eine gubernative Entscheidung gestützt werden kann.

1076) *A. K.*, Protokoll-Nr. 64 I, S. 100.

> „So dürfen nachrichtendienstliche Aktivitäten mit Eingriffscharakter im Inland nur durch die deutschen Nachrichtendienste durchgeführt werden. Ein fremder Dienst kann hier nur zur Unterstützung und in Zusammenarbeit mit einem deutschen Staatsorgan tätig werden, und zwar ausschließlich zur gesetzlichen Aufgabenerfüllung der deutschen Nachrichtendienste.“[1077]

e) Ausstattung von Mitarbeiter_innen der US-Dienste mit deutschen Tarnpapieren

DIA-Befrager_innen wurden für ihre Arbeit bei der HBW mit deutschen Tarnpapieren ausgestattet, die sie bis zu ihrer Versetzung behielten. In Befragungen waren sie ebenfalls als HBW-Mitarbeiter_innen legendiert,[1078] es war den Befragten also nicht bewusst, dass sie nicht nur vor deutschen, sondern auch vor US-amerikanischen Sicherheitsbehörden aussagten.

Die Ausstattung von Mitarbeiter_innen der US-Dienste mit deutschen Tarnpapieren erfolgte nach Angaben der Bundesregierung auf Grundlage des § 3 BNDG i.V.m. § 8 Abs. 2 BVerfSchG.

Nach § 3 BNDG darf der BND zur heimlichen Beschaffung von Informationen einschließlich personenbezogener Daten die Mittel gemäß § 8 Abs. 2 BVerfSchG anwenden, wenn Tatsachen die Annahme rechtfertigen, dass dies zur Erfüllung seiner Aufgaben erforderlich ist.

§ 8 Abs. 2 Satz 1 bis 3 BVerfSchG lautet:

> „Das Bundesamt für Verfassungsschutz darf Methoden, Gegenstände und Instrumente zur heimlichen Informationsbeschaffung, wie den Einsatz von Vertrauensleuten und Gewährspersonen, Observationen,

---

1077) Leiterin des Fachbereichs Nachrichtendienste an der Fachhochschule des Bundes für öffentliche Verwaltung *Monika Rose-Stahl*: Recht der Nachrichtendienste, 2002, S. 111, http://www.fhbund.de/nn_15672/SharedDocs/Publikationen/50__Publikationen/15__Beitraege__Innere__Sicherheit/band__18,templateId=raw,property=publicationFile.pdf/band_18.pdf (abgerufen am 15. Juni 2017).

1078) *A. K.*, Protokoll-Nr. 64 I, S. 18.

> Bild- und Tonaufzeichnungen, Tarnpapiere und Tarnkennzeichen anwenden. In Individualrechte darf nur nach Maßgabe besonderer Befugnisse eingegriffen werden. Im Übrigen darf die Anwendung eines Mittels gemäß Satz 1 keinen Nachteil herbeiführen, der erkennbar außer Verhältnis zur Bedeutung des aufzuklärenden Sachverhalts steht.“

Geht man davon aus, dass die HBW als Legendenbehörde selbst das Mittel zur heimlichen Beschaffung von Informationen im Sinne des § 3 BNDG war, so war die Ausstattung von Mitarbeiter_innen der US-Dienste mit deutschen Tarnpapieren ein Mittel zum Schutze des Mittels zur heimlichen Beschaffung von Informationen. Es ist aber äußerst zweifelhaft, ob eine solche doppelte Ableitung noch von dem Regelungsgedanken des § 3 BNDG i.V.m. § 8 Abs. 2 BVerfSchG gedeckt ist. Dies inbesondere vor dem Hintergrund des Rechtsstaatsprinzips im Hinblick auf die Tatsache, dass in den Befragungen der HBW die Mitarbeiter_innen der AND als Vertreter_innen einer deutschen Behörde aufgetreten sind.

f) Fachaufsicht im Kanzleramt lange Zeit untätig

Die zuständige Rechts- und Fachaufsicht im Bundeskanzleramt reagierte reichlich spät auf die rechtswidrige Befragungspraxis der BND-Tarnbehörde.

Erst Ende November 2013, ungefähr ein halbes Jahr vor Auflösung der HBW, untersagte der verantwortliche Referatsleiter der Fachaufsicht, *Albert Karl*, die Durchführung von alleinigen Befragungen durch Partnerdienste. In einer E-Mail vom 25. November 2013 an die BND-Leitung wies *Karl* an, dass ab sofort keine Befragungen mehr ohne Beisein von BND-Mitarbeiter_innen stattfinden dürften.[1079]

Aus einem durch den Referatsleiter des BND angeforderten Bericht habe er von den alleinigen AND-Befragungen erfahren.[1080] Davor habe er nichts Konkretes über die Befragungspraxis der HBW gewusst.[1081]

1079) *Karl*, Protokoll-Nr. 76 I, S. 73.

1080) *Karl*, Protokoll-Nr. 76 I, S. 75.

1081) *Karl*, Protokoll-Nr. 76 I, S. 73.

Es ist auch an dieser Stelle fraglich, welches Verständnis von Aufsicht die für die Geheimdienstkontrolle zuständigen Referate im Bundeskanzleramt zu diesem Zeitpunkt gehabt haben. Offensichtlich wurden entsprechende Nachforschungen erst angestellt, nachdem die Diskussion um die problematischen HBW-Befragungen bereits die Öffentlichkeit erreicht hatte. Seine Kontrollfunktion gegenüber dem BND hatte das Kanzleramt auch hier die längste Zeit versäumt.

2. Kooperation der HBW mit dem Bundesamt für Migration und Flüchtlinge

Im Untersuchungsausschuss wurde auch die Zusammenarbeit der HBW mit dem BAMF[1082] diskutiert.

a) Auswahl per Kriterienkatalog

Das BAMF, eigentlich für die Bearbeitung von Asylanträgen zuständig, unterstützte die HBW regelmäßig bei der Auswahl der zu befragenden Einwanderer_innen.

Das Bundesamt traf hierbei nach der Anhörung auf Grundlage eines „Kriterienkatalogs“ der HBW die Vorauswahl für die Befragungen. Die Zeugin *Renate Leistner-Rocca*, langjährige BAMF-Mitarbeiterin und bis 2013 Leiterin des Sicherheitsreferats, schilderte die Auswahlpraxis folgendermaßen:

> „Die Entscheider hatten alle diesen Kriterienkatalog des BND und auch des Verfassungsschutzes, und wenn im Verlauf eines Asylverfahrens, insbesondere im Verlauf einer Anhörung, Schilderungen kamen, wo die Kollegen angenommen haben, dass es unter diesen Kriterienkatalog oder unter ein, zwei Stichworte der Kriterienkataloge zu subsummieren ist, dann haben die Kollegen uns diesen Fall geschickt. Also, mit „uns“ meine ich jetzt das Sicherheitsreferat. Meine Kollegen haben sich den Fall dann noch mal angesehen und haben dann entschieden, ob das Anhörungsprotokoll weitergegeben wird und an wen.“[1083]

1082) Bis 2004 Bundesamt für die Anerkennung ausländischer Flüchtlinge.

1083) *Leistner-Rocca*, Protokoll-Nr. 76 I, S. 12.

Sprachen Asylbewerber_innen in ihrer Erstanhörung über Themen wie organisierte Kriminalität, terroristische Gruppierungen, Waffenhandel oder auch staatliche Administration oder das Militär, wurden diese „Fälle" an das Sicherheitsreferat weitergeleitet und nach einer Überprüfung dann an die HBW.[1084]

In späteren Jahren habe das Sicherheitsreferat sogenannte „Montagslisten" für die HBW zusammengestellt:

> „Wir haben von unserem Statistikreferat uns jeden Montag eine Liste mit angehörten Asylbewerbern aus bestimmten Herkunftsländern geben lassen. Die Liste haben wir dann noch mal aussortiert nach Altersgruppen, haben uns die Liste noch kurz angesehen und haben die Daten an die HBW oder an den BND dann weitergegeben."[1085]

Die Weitergabe erfolgte meistens direkt an den Verbindungsbeamten der HBW, der sein Büro auf dem gleichen Gang wie das Sicherheitsreferat hatte. [1086] Rechtsgrundlage für die Datenweiterleitung sei § 8 Abs. 3 BNDG gewesen, so *Leistner-Rocca*.[1087]

b) Freiwillige Kooperation mit einer Tarnbehörde?

Dem BAMF war bewusst, dass die HBW eine Tarneinrichtung des BND war.[1088] Den befragten Asylbewerber_innen jedoch war nicht klar, dass sie von einem Geheimdienst befragt wurden. Die Befragungen fanden unter der Legende HBW statt.[1089] Da im Untersuchungsausschuss nur Befrager_innen und nicht Befragte vernommen wurden, fand die Perspektive Letzterer im Ausschuss kaum Platz. Aus der Reportage „Geheimer Krieg" geht hervor, dass den Asylbewerber_innen häufig nicht klar war, welcher Behörde gegenüber sie gerade aussagten.[1090] Ein somalischer Dolmetscher berichtet,

---

1084) *Leistner-Rocca*, Protokoll-Nr. 76 I, S. 13; vgl. Kriterienkatalog des BND, Stand: März 2004, MAT A BAMF-3/1, Bl. 40 f. (VS-NfD).

1085) *Leistner-Rocca*, Protokoll-Nr. 76 I, S. 12.

1086) *A. K.*, Protokoll-Nr. S. 64 I, S. 86.

1087) *Leistner-Rocca*, Protokoll-Nr. 76 I, S. 17.

1088) *A. K.*, Protokoll-Nr. 64 I, S. 50.

1089) *A. K.*, Protokoll-Nr. 64 I, S. 78.

1090) Vgl. *Christian Fuchs/John Goetz*: „Geheimer Krieg", 1. Auflage, November 2013, S. 122 ff.

nicht selten seien schon bei der offziellen Asylanhörung neben den BAMF-Befrager_innen zusätzliche Personen anwesend gewesen, die sich als Praktikanten ausgaben und alle Aussagen der Asylbewerber_innen auf ihren Laptops mitschrieben.[1091]

> „„Für viele Somalier ist das der wichtigste Tag in ihrem Leben‘, sagt *Ahmed Wazir*. ‚An dem Tag legen sie ihr Schicksal auf den Tisch und eine Person kann über ihre Zukunft entscheiden. Viele zittern, wenn ich sie in den Raum führe.‘ Die zusätzlichen Personen bei dem Interview fallen ihnen meistens durchaus auf, niemals würden sie sich jedoch trauen, ihre Anwesenheit in Frage zu stellen.“[1092]

Falls die Befragten Angaben von entsprechendem Interesse machten, erfolge dann die Kontaktaufnahme durch die HBW. Der Zeuge *R. C.* gab an, Grundlage für die Einladung der Asylbewerber_innen zu einem Gespräch sei das Anhörungsprotokoll.[1093]

Zu Beginn des Erstgesprächs seien die Befragten informiert worden, die Befragung erfolge freiwillig und habe keinerlei Einfluss auf ihr Asylverfahren.[1094]

Wie frei der Wille der befragten Asylbewerber_innen tatsächlich war, ist zweifelhaft. Mitten im Asylverfahren von einer staatlichen Behörde darum gebeten zu werden, sich „zu einem Gespräch zur Verfügung zu stellen“ dürfte wohl angesichts der Zwangslage in der sich die Gefragten befinden, schwer abzulehnen seien:

> „Viele der Befragten sind der Einladung des Geheimdienstes nur gefolgt, weil sie Angst vor Nachteilen hatten, wenn sie nicht hingegangen wären.“[1095]

Es ist grundsätzlich fragwürdig, von einer Einwilligung zu sprechen, wenn den Befragten nicht mitgeteilt wurde, dass sie mit einem Geheimdienst (oder sogar mehreren)

1091) *Christian Fuchs/John Goetz*: „Geheimer Krieg“, 1. Auflage, November 2013, S. 123.

1092) *Christian Fuchs/John Goetz*: „Geheimer Krieg“, 1. Auflage, November 2013, S. 123.

1093) *R. C.*, Protokoll-Nr. 110 I, S. 11.

1094) *R. C.*, Protokoll-Nr. 110 I, S. 11.

1095) *Christian Fuchs/John Goetz*: „Geheimer Krieg“, 1. Auflage, November 2013, S. 130.

kooperierten und die von ihnen gemachten Angaben ohne ihr Wissen an ausländische Nachrichtendienste weitergegeben wurden. Laut Aussagen der Zeugin *A. K.* sei die HBW gegenüber den Befragten auch während und nach der Befragung nicht als BND-Behörde offengelegt worden.[1096] Ob die Befragten im gleichen Umfang Informationen preisgegeben hätten, wenn sie gewusst hätten, dass diese geheimdienstlich und militärisch verwertet werden würden, muss bezweifelt werden.

c) Schutz der Befragten

Die Kooperation der Befragten mit dem BND, wenn auch legendiert und den Befragten meistens selbst nicht bewusst, stellte eine potenzielle Gefährdung für sie dar. Das sah auch die HBW selbst so, wodurch es teilweise zu Interventionen der Behörde beim BAMF kam. Um die Befragten nicht der Gefahr auszusetzen, im Herkunftsland aufgrund der Kooperation mit einem Geheimdienst des Verrats bezichtigt zu werden,[1097] prüfte das BAMF in diesen Fällen den Tatbestand der Nachfluchtgründe. Das Sicherheitsreferat des BAMF führte dazu aus:

„[redacted][1098]

Die Intervention durch die HWB fand jedoch nicht grundsätzlich statt, sondern nur in Fällen, in denen der Geheimdienst ein besonderes „Interesse an einer bestimmten Person“[1099] hatte, also „[w]enn sich herauskristallisiert hat, dass Wissen vorhanden ist,

1096) *A. K.*, Protokoll-Nr 67 I, Teil 2, S. 30.

1097) *Leistner-Rocca*, Protokoll-Nr. 76 I, S. 29.

1098) Unterrichtungsvorlage des Sicherheitsreferates für den Präsidenten des BAMF vom 26. März 2009, MAT A BAMF-1b, Bl. 36 (37 f.), (VS-NfD).

1099) *R. C.*, Protokoll-Nr. 110 I, S. 23.

das in einem längeren Stadium abgeschöpft werden muss“[1100]. Je wichtiger die Informationen, desto höher die Chance, entsprechend geschützt zu werden.

Dass die betreffenden Personen nicht nur im Herkunftsland gefährdet sein könnten, sondern auch in Deutschland – teilweise ohne ihr Wissen – wurde dabei offenbar in Kauf genommen.

3. Befragungen bis heute

Dass die HBW offiziell im Sommer 2014 aufgelöst wurde, scheint nicht das endgültige Ende der Befragungen zur Folge gehabt zu haben. Presseberichten zufolge wurden auch nach Abwicklung der Tarnbehörde weiterhin Asylbewerber_innen befragt:

> „[…] später bekräftigte die damalige Leiterin der BND-Abteilung in einer ‚Quartalsbesprechung‘ mit dem BAMF, dass zwar die Stellen für das ‚Befragungswesen‘ minimiert würden und es zur Umstrukturierung innerhalb des BND komme, alles aber bei ‚gleichbleibender Aufgabenstellung‘. Das Abschöpfen von Flüchtlingen sollte weitergehen.“[1101]

Während der Befragung der Zeugin *A. K.* zu Verbindungsbeamten der HBW beim BAMF merkte *Torsten Akmann* (BMI) an, auch nach der Abwicklung der HBW habe es Verbindungsbeamte des BND beim BAMF gegeben.[1102]

Auf eine Kleine Anfrage der Fraktion DIE LINKE. zu BND-Befragungen von Asylsuchenden im Dezember 2016 antwortete die Bundesregierung:

> „Seit Ende Oktober 2015 befragt der BND vereinzelt Flüchtlinge im Inland. Diese Befragungen werden jedoch ausschließlich unter Offen-

1100) *R. C.*, Protokoll-Nr. 110 I, S. 23.

1101) *Die Zeit* vom 14. Januar 2016, Nr.3, S. 12: „Informant Flüchtling“.

1102) *A. K.*, Protokoll-Nr. 64 I, S. 107.

> legung des BND-Hintergrunds, auf Basis der Freiwilligkeit, ohne Beteiligung ausländischer Nachrichtendienste und nur nach Klärung des Asylstatus durchgeführt. […]“[1103]

Das deckt sich mit Medienberichten darüber, dass sowohl der BND als auch das BfV immer noch oder wieder Asylbewerber_innen befragen.[1104] So ergaben die Recherchen der Journalisten, dass die Nachrichtendienste auch gegenwärtig in Erstaufnahmelagern anwesend sind: In Zirndorf fanden sie ein besetztes BND-Büro, in Friedland einen Mitarbeiter des Verfassungsschutzes.[1105]

1103) Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. vom 7. Dezember 2016, Bundestagsdrucksache 18/10585, S. 11.

1104) Vgl. auch netzpolitik.org – „Internes Papier des Innenministeriums: Verfassungsschutz darf direkt an Asylanhörungen teilnehmen“, https://netzpolitik.org/2016/internes-papier-des-innenministeriums-verfassungsschutz-darf-direkt-an-asylanhoerungen-teilnehmen/ (abgerufen am 1. Juni 2017).

1105) *Die Zeit* vom 14. Januar 2016, Nr. 3, S. 12: „Informant Flüchtling“.

XII. Geheimer Krieg – Die Beteiligung Deutschlands am US-Drohnenkrieg

1. Kernfrage der Befassung des Untersuchungsausschusses: Ist Deutschland beteiligt am US-Drohnenkrieg?

Bereits im Frühjahr 2012 gab es Pressemeldungen über einen Vorstoß der *Vereinigung Juristen gegen atomare, biologische und Chemische Waffen* (*IALANA*) gegen die Nutzung des US-Stützpunkts Ramstein für „exzessive Kriegsführung“ wie gezielte Tötungen durch die USA mittels unbemannter Drohnen. Die Vereinigung forderte das Bundesverteidigungsministerium auf, den Betrieb in Ramstein zu überwachen und verlangte Auskunft über die von dort ausgehenden Flüge.[1106]

Im Frühjahr 2013 gab es erstmals Berichte in der deutschen Presse, wonach die US-Luftwaffenbasis auf der Militärbasis Ramstein ein zentraler Dreh- und Angelpunkt des US-Drohnenkrieges sei.[1107] Parlament, Presse und Öffentlichkeit stellten umgehend dringliche Fragen. Auf Fragen zur Rolle Ramsteins für den US-Drohnenkrieg antwortete die Bundesregierung jahrelang lediglich, dass die US-Regierung versichert hätte, dass sie „keine“ bzw. „keine eigenen gesicherten“ Erkenntnisse habe und dass die amerikanische Seite versichert habe, geltendes Recht würde eingehalten.

So antwortete der Staatsekretär *Dr. Braun* am 27. März 2013 auf die Frage, inwieweit nach Kenntnis der Bundesregierung Einrichtungen der NATO und des US-Militärs in Deutschland (z. B. Airbase Ramstein, AFRICOM in Stuttgart) jeweils an Zielauswahl oder Durchführung von bewaffneten Drohneneinsätzen im Ausland beteiligt sind: „Der Bundesregierung liegen keine Erkenntnisse zu von US-Streitkräften oder NATO-Einrichtungen in der BRD geplanten oder durchgeführten Drohneneinsätzen vor.“[1108]

Auf Vorhalt von Berichten im TV-Magazin *Panorama* und der *Süddeutschen Zeitung* vom 30./31. Mai 2013 antwortete die Staatsministerin *Pieper* am 12. Juni 2013 auf die Frage, ob die Bundesregierung ausschließe, dass in US-Einrichtungen in Deutschland – etwa auf der Ramstein Air Base oder bei AFRICOM in Stuttgart – gezielte Tötungen

1106) *Neues Deutschland* vom 24. März 2012, „Luftdrehkreiz für den Krieg“.

1107) *Das Erste, Panorama* vom 30. Mai 2013, „US-Drohnenkrieg läuft über Deutschland“, http://daserste.ndr.de/panorama/archiv/2013/US-Drohnenkrieg-laeuft-ueber-Deutschland,ramstein109.html [letzter Abruf: 9. Juni 2017].

1108) Bundestagsdrucksache 17/12949.

mittels Drohnen in Afrika, u. a. in Somalia, geplant, durchgeführt und unterstützt werden:

> „Der Bundesregierung liegen keine eigenen gesicherten Erkenntnisse zu von US-Streitkräften in der Bundesrepublik Deutschland angeblich geplanten oder geführten Einsätzen vor."

Und weiter:

> „Trotzdem kann ich Ihnen an dieser Stelle nur sagen, dass der Bundesregierung dazu keine Erkenntnisse vorliegen und dass Außenminister Westerwelle zuletzt bei seinem Besuch in den USA beim Zusammentreffen mit dem Außenminister *John Kerry* auch über dieses Thema gesprochen hat. Der amerikanische Außenminister hat ihm versichert, dass jedwedes Handeln der USA, auch auf deutschem Staatsgebiet, streng nach den Regeln des Rechts erfolgt."[1109]

Am 19. Juni 2013 hat US-Präsident *Obama* bei seinem Besuch in Berlin betont, dass von deutschem Boden keine Drohnen zu Kampfeinsätzen starten bzw. nicht geführt und gesteuert würden.[1110] Dies entsprach den Auskünften, die von US-Militärs und der US-Regierung den Medien und der Öffentlichkeit auf zahlreiche Anfragen gegeben wurden. Es war die US-Sprachregelung, die in der einen oder anderen Variante stets eingehalten und dann auch von der Bundesregierung übernommen wurde.

Diese Antworten lagen allerdings neben den Fragen und der Sache. Sie enthielten Erklärungen zu Teilen der Fragen oder zu Fragen, die so gar nicht gestellt waren. Sie waren daher nicht nur unvollständig, sondern auch falsch. Dies ganz abgesehen davon, dass auch Zweifel begründet sind, dass die Antworten der Wahrheit entsprachen.

So wurde von den Abgeordneten[1111] nicht nur nach Planung und Führung bzw. Befehligen oder Starten der Drohneneinsätze von der US-Air Base in Ramstein oder von

---

1109) Antwort auf mündliche Frage des Abgeordneten *Hans-Christian Ströbele*, Bundestags-Plenarprotokoll 17/245.

1110) Rede von Präsident *Obama* am 19. Juni 2013 in Berlin, nachzulesen unter: http://www.spiegel.de/politik/deutschland/obamas-rede-in-berlin-am-19-juni-2013-im-wortlaut-englisch-a-906741.html [letzter Abruf: 13. Juni 2017].

1111) Vgl. u. a. Antworten der Bundesregierung auf die Kleinen Anfragen der Fraktion Bündnis90/DIE GRÜNEN „Hinweise auf völkerrechtswidrige Praktiken der USA von deutschem Staatsgebiet aus und die diesbezüglichen Kenntnisse der Bundesregierung", Bundestagsdrucksache 18/237; der Fraktion DIE LINKE. „Die Rolle des United Staates Africa Commands

AFRICOM in Stuttgart ausgefragt, sondern nach der Beteiligung an „Zielauswahl oder Durchführung“ bzw. ob gezielte Tötungen mittels Drohnen in diesen US-Einrichtungen „geplant, durchgeführt, unterstützt“ werden. Die Fragen nach „beteiligen“ bzw. „unterstützen“ wurden genauso wenig beantwortet wie jene, ob die Bundesregierung die Unterstützung ausschließen kann. Unter diese Begriffe fallen aber jegliche Arten von Involvierung, Verstrickung und Beihilfe beim Einsatz der Kampfdrohnen – auch die Steuerung über Relaisstationen in Ramstein, zumal wenn diese Unterstützung unverzichtbar und unersetzbar für das Erreichen des Zieles der gezielten Tötung ist, weil die tatsächlichen Gegebenheiten (hier die Erdkrümmung) einer direkten Steuerung über Satelliten von den USA aus entgegensteht. Erfragt wurde also ersichtlich auch, ob der Einsatz der US-Kampfdrohnen in anderen Länder mit Hilfe oder „über“ Ramstein gesteuert und dirigiert wurden und werden, um die Ziele ausfindig machen, genau zu orten und die Raketen zur Tötung abzufeuern.

Für Bundesregierung und US-Stellen war bei all den vielen Fragesteller_innen aus Öffentlichkeit und Parlament erkennbar, dass diese sich um die Funktion und Rolle Ramsteins sorgten – und weil diese US-Einrichtung auf deutschem Boden liegt, auch um die Verstrickung Deutschlands bei US-Drohneneinsätze insgesamt – insbesondere ob dort möglicherweise über den Tod von Menschen außerhalb von Gerichtsverfahren mitentschieden oder dieser anderweitig von deutschem Boden aus beeinflusst wurde. Um die Beantwortung dieser konkreten Fragen drückte sich die Bundesregierung jedoch bewusst und gezielt herum trotz jahrelangem und detailliertem Nachhaken. Sie verletzte nachhaltig die gesetzlich garantierten Informations- und Kontrollrechte von Bundestag und Öffentlichkeit. Deshalb wurde in der Folge eine Befassung des Untersuchungsausschusses mit dieser dringlichen Frage erforderlich. Diese ergab, dass die Annahmen und Befürchtungen berechtigt waren, dass Deutschland in den geheimen Drohnenkrieg der USA, von dem sich die Bundesregierung öffentlich lange distanzierte, zutiefst verstrickt war und vermutlich nach wie vor ist.

---

und der US-Militärbasis in Ramstein für US-Drohnenangriffe“, Bundestagsdrucksache 18/2794; „Die US-Basis Ramstein als wichtiger Knoten im weltweiten Drohnenkrieg“, Bundestagsdrucksache 18/11023 und „Zur Rolle des in Deutschland stationierten United States Africa Command bei gezielten Tötungen durch US-Streitkräfte in Afrika“, Bundestagsdrucksache 17/14401.

2. Der US-Drohnenkrieg: Zahlen und Fakten

Der Einsatz von Drohnen durch die *USA* zur gezielten Tötung von Menschen in Ländern, in denen die *USA* sich eigentlich nicht im Krieg befindet, ist zu einem Markenzeichen der US-Anti-Terror-Strategie geworden.

Insbesondere in Pakistan, dem Jemen und Somalia, aber auch in anderen Ländern Afrikas und des Nahen Ostens sind durch US-Drohnenangriffe seit 2002 nach Schätzungen von renommierten Nichtregierungsorganisationen wie dem *Bureau of Investigative Journalism* insgesamt mindestens 1.400 Zivilist_innen getötet worden.. Es wird angenommen, dass es sich bei bis zu 300 der Opfer um Kinder handelt.[1112] Offizielle Statistiken hat die US-Regierung nie aufgestellt. Eine formelle Entschuldigung haben die Angehörigen der vielen zivilen Opfer nie erhalten. Es gibt keine offiziellen Entschädigungszahlungen an die Hinterbliebenen, denen häufig mit der Tötung des Vaters in patriarchalen Strukturen keine Lebensgrundlage bleibt.

Der Alltag der Menschen, die konstant mit der Präsenz der Drohnen leben, ist von ständigem Schrecken erfüllt.[1113] Niemand weiß, wer als nächstes Ziel oder (Mit-)Betroffene_r eines Angriffs wird. Schon ein irgendwie geartetes verdächtiges Verhalten kann einen tödlichen Drohnenangriff auslösen. Doch was ein solches Verhalten ausmacht, weigern sich die Verantwortlichen der US-Regierung zu sagen. Bei dem Versuch, terrorverdächtige Personen zu identifizieren, werden auch demographische Daten verwendet. Dementsprechend sind männliche Personen im Alter von teilweise schon 12 bis 65 Jahren besonders von Drohnenangriffen bedroht. Laut US-Regierung werden Männer dieser Altersklasse in Ländern wie dem Jemen oder bestimmten Regionen Pakistans nicht als Zivilisten betrachtet, es sei denn, sie können ihre Unschuld beweisen – posthum.[1114] Derartige Nachforschungen werden jedoch auch posthum

1112) *Bureau of Investigative Journalism*, „Drone Warfare”, https://www.thebureauinvestigates.com/projects/drone-war (abgerufen am 02.06.2017).

1113) *Reprieve*, „Americas deadly drones programme”, http://www.reprieve.org.uk/case-study/drone-strikes/ (abgerufen am 02.06.2017).

1114) *Reprieve*, „Americas deadly drones programme”, http://www.reprieve.org.uk/case-study/drone-strikes/ (abgerufen am 02.06.2017).

durch die *USA* selber nicht durchgeführt. Es erfolgt keine Rehabilitation oder eine Entschädigung der Angehörigen.

Der Einsatz von Drohnen wird von US-Vertreter_innen vor allem damit begründet, dass es sich dabei um eine extrem präzise Waffe handele und auf diese Weise sogenannte „Kollateralschäden" – also Tötungen von Zivilist_innen – weitestgehend vermieden würden. Dabei ist das Gegenteil der Fall. Unabhängige Expert_innen haben in langjährigen Recherchen feststellen müssen, dass die Zielbestimmung bei Drohneneinsätzen in der Praxis sehr unpräzise sei. Schon im Jahr 2014 belegten Anwält_innen der Menschenrechtsorganisation *Reprieve*, dass bei Drohnenangriffen auf nur 41 mutmaßliche Terroristen in Pakistan und dem Jemen insgesamt bis zu 1.147 Menschen getötet wurden.[1115] Dabei deutet vieles darauf hin, dass einige der vermeintlich gezielt getöteten Männer noch am Leben sind.[1116]

Nach Meinung der US-Regierung befindet sie sich seit dem Angriff auf das World Trade Center am 11. September 2001 in einem globalen Krieg gegen den Terrorismus (*„global war on terror*"). Die US-Regierung rechtfertigt ihr Drohnenprogramm mit der Begründung, dass es juristisch von Art. 51 UN-Charta, dem Recht auf Selbstverteidigung, gedeckt sei und sie so mutmaßliche Terroristen töten dürfe, egal wo auf der Welt sie sich befänden. Dass dem nicht so ist und jede Beteiligung am US-Drohnenkrieg damit ebenfalls rechtswidrig ist, zeigt dieses Kapitel unter XII.5. (Rechtliche Verantwortung der Bundesregierung für den US-Drohnenkrieg).

1115) *Reprieve*, „You never die twice: Multiple kills in the US drone program", Executive Summary, November 2014, http://www.reprieve.org/wp-content/uploads/2014_11_24_PUB-You-Never-Die-Twice-Multiple-Kills-in-the-US-Drone-Program-1.pdf (abgerufen am 02.06.2017); The Guardian „41 men targeted but 1,147 people killed: US drone strikes – the facts on the ground", 24.11.2014, https://www.theguardian.com/us-news/2014/nov/24/-sp-us-drone-strikes-kill-1147 (abgerufen am 02.06.2017).

1116) *Reprieve*, „You never die twice: Multiple kills in the US drone program", Executive Summary, November 2014, http://www.reprieve.org/wp-content/uploads/2014_11_24_PUB-You-Never-Die-Twice-Multiple-Kills-in-the-US-Drone-Program-1.pdf (abgerufen am 02.06.2017); The Guardian „41 men targeted but 1,147 people killed: US drone strikes – the facts on the ground", 24.11.2014, https://www.theguardian.com/us-news/2014/nov/24/-sp-us-drone-strikes-kill-1147 (abgerufen am 02.06.2017).

3. Die Rolle Deutschlands im US-Drohnenkrieg

„We track ‘em you whack ‘em“ – „Wir spüren sie auf, ihr nietet sie um“ – so beschrieb die *NSA* laut Zeuge *Thomas Drake* das US-Drohnenprogramm.[1117]

Bereits in der ersten Zeugenvernehmung des *NSA*-Untersuchungsausschusses Anfang Juli 2014 kam die zentrale Rolle Deutschlands im Drohnenkrieg zur Sprache. Der ehemalige leitende Angestellte der *NSA* und mittlerweile als Whistleblower bekannte *Thomas Drake* verwies in seiner Aussage darauf, dass Deutschland „eine […] Plattform für alle Arten von nachrichtendienstlichen Operationen“[1118] sei.

So sei es der zentrale Standort, um Drohneneinsätze in verschiedenen Konfliktgebieten zu ermöglichen:

> „Eine der primären Plattformen – das sage ich hier nur –, die eingesetzt wurde, um das zu ermöglichen, war Deutschland. [...]“[1119]

Drake deutete an, dass Deutschland zum einen als Plattform zur Steuerung unbemannter Flugobjekte diene und zum anderen nachrichtendienstliche Informationen an die NSA weitergebe, die zur Lokalisierung von Zielpersonen der Angriffe dienten:

> „Sie [die Bush-Administration] operieren auf deutschem Boden, liefern aber auch Informationen an andere Einrichtungen, um Drohnen zu steuern.“[1120]

> „Man brauchte Orte, an denen man diese Drohnen bedienen und auch die nachrichtendienstlichen Informationen zur Verfügung stellen konnte. Angesichts der Beschaffenheit gewisser Einrichtungen in Deutschland, kann man sagen – auf Grundlage der Kenntnisse, die ich hatte; Sie sprachen von schmutzigem Wissen –, dass Deutschland

---

1117) *Drake*, Protokoll-Nr. 11 I, S. 175.

1118) *Drake*, Protokoll-Nr. 11 I, S. 175.

1119) *Drake*, Protokoll-Nr. 11 I, S. 175.

1120) *Drake*, Protokoll-Nr. 11 I, S. 175.

> selbst dazu benutzt wurde, verfassungswidrig, die eigene Sicherheitsbehörde, um bei der Ausführung dieser Art von Operationen zu helfen.“[1121]

a) Ramstein als Zentrum des US-Drohnenkrieges in Europa

Ein dreiviertel Jahr später, im April 2015, veröffentlichte die Online-Zeitung *The Intercept* in Kooperation mit *Der Spiegel* Grafiken aus den Snowden-Dokumenten, die den US-Luftwaffenstützpunkt Ramstein als „Herz“ des US-Drohnenprogramms ausmachen. Ramstein diene als Satelliten-Relaisstation, über die vom Südwesten der USA aus Drohnen in Jemen, Somalia, Afghanistan und anderen Staaten gesteuert würden, so *The Intercept*.[1122]

Die US-Militärbasis in Rheinland-Pfalz sei das Zentrum der Kommunikationsinfrastruktur für Drohnenangriffe, zitiert der Artikel den Drohnen-Experten *Dan Gettinger*. Ramstein habe in seiner Funktion damit mehr Bedeutung als die Waffe, die die Kampfdrohne mit sich trägt, fasst *Gettinger* zusammen.[1123]

Die in den veröffentlichten Grafiken erkennbaren Informationen weisen ebenfalls auf die zentrale Rolle Ramsteins hin.[1124]

Das bestätigte auch die Aussage des Zeugen *Brandon Bryant* im Untersuchungsausschuss. Der ehemalige „Sensor Operator“, quasi ein Drohnen-Co-Pilot, hatte von 2006 bis 2011 für die US-Air Force Drohneneinsätze im Irak, Afghanistan, Pakistan, Somalia und Jemen geflogen.[1125] Dann verließ er das Militär und wurde zum Whistleblower, der fortan die Öffentlichkeit über den US-Drohnenkrieg aufklärte. *Bryant* hatte bereits im

---

1121) *Drake*, Protokoll 11 I, S. 175.

1122) Siehe https://theintercept.com/2015/04/17/ramstein/ (19. Mai 2017): „U.S. intelligence document obtained by The Intercept confirms that the sprawling U.S. military base in Ramstein, Germany serves as the high-tech heart of America's drone program. Ramstein is the site of a satellite relay station that enables drone operators in the American Southwest to communicate with their remote aircraft in Yemen, Somalia, Afghanistan and other targeted countries.“

1123) Siehe https://theintercept.com/2015/04/17/ramstein/ (19. Mai 2017): „Ramstein is the focal point for drone communications,” says Dan Gettinger, co-director of the Center for the Study of the Drone at Bard College. „If the communications infrastructure didn't exist, the drone would be just a remote control plane, a toy basically.” It is „more important to the drone operations than the weapons a drone carries.”

1124) MAT A Sek-21b, Bl. 1.

1125) *Bryant*, Protokoll-Nr. 67 I, S. 94.

Jahr 2013 mehrere Interviews gegeben, in denen er von seinen Erfahrungen mit dem Drohnenprogramm berichtete und bis dahin unbekannte Insider-Informationen über die genauen Abläufe von Operationen mit Drohnen preisgab.[1126]

Bryant ging bei seiner Vernehmung im Oktober 2015 auch auf die Rolle Deutschlands im Geheimen Krieg der Vereinigten Staaten ein.

Drohneneinsätze seien „Remote Split Operations", was bedeute, dass die unbemannten Luftfahrzeuge von den Vereinigten Staaten aus gesteuert würden, obwohl die Operation in einem anderen Land stattfinde. Drohnen in Nahost beispielsweise würden über Satellitensignale von den USA aus gesteuert, so *Bryant*. Dabei sei Ramstein zentral eingebunden:

> „Ich denke, es wird Sie interessieren, dass es die Ramstein Air Force Base ist, die uns dazu in die Lage versetzt hat als Signalrelais nach Nahost von den Vereinigten Staaten."[1127]

Denn für die Durchführung der Operationen im Nahen und Mittleren Osten und auf dem afrikanischen Kontinent ist das US-Militär auf eine Relaisstation in Europa angewiesen, da Satellitensignale aus den USA aufgrund der Erdkrümmung die unbemannten Luftfahrzeuge nicht direkt erreichen können.

Zwar würden Drohnen nicht von Ramstein aus gesteuert[1128], aber, erläuterte *Bryant*:

> „Also, alle Daten aus Nahost und Afrika laufen über Ramstein, über das Relais. Alles, was mit Drohneneinsätzen zu tun hat, diese Daten laufen über Ramstein."[1129]

1126) Vgl. http://www.gq.com/story/drone-uav-pilot-assassination; http://edition.cnn.com/2013/10/23/us/drone-operator-interview/index.html; http://www.zeit.de/politik/ausland/2013-10/usa-drohnen-pilot; http://www.sueddeutsche.de/politik/us-drohnenkrieg-immer-fliessen-die-daten-ueber-ramstein-1.1929160 (abgerufen am 19. Mai 2017).

1127) *Bryant*, Protokoll-Nr. 67 I, S. 23.

1128) *Bryant*, Protokoll-Nr. 67 I, S. 23.

1129) *Bryant*, Protokoll-Nr. 67 I, S. 65.

Bryant betonte mehrfach die technische Bedeutung der Militärbasis als „Glied in der Kette“[1130] der „Remote Split Operations“:

> „Alle Daten – jedes einzelne Bit an Daten und Infomationen –, die zwischen dem Fluggerät und der Flugmannschaft übertragen wurden, liefen über die Ramstein Air Force Base.“[1131]

Von Ramstein gebe es, so die Darstellung *Bryants*, eine direkte Glasfaserverbindung zum Pentagon, über die alle von Drohnen gesammelten Daten in die USA weitergeleitet würden.[1132]

Einige der von *The Intercept* veröffentlichen Grafiken zeigen auch eine durchgehende Glasfaserverbindung zwischen Ramstein und der Creech Air Force Base in Nevada in den USA, wo die Steuerung vieler Drohnenoperationen stattfindet und von der aus *Bryant* den Großteil seiner Drohneneinsätze flog.

Neben der Satellitenrelais-Station beherbergt Ramstein auch ein sogenanntes „Distributed Ground System“ (DGS) sowie ein sogenanntes „Air and Space Operations Center“ (AOC),[1133] in dem Bildanalyst_innen Daten aufbereiten, die dann wiederum den Entscheidungen für oder gegen einen Waffeneinsatz zu Grunde gelegt werden.[1134]

Letzteres ist für Luftoperationen der US-Militärkommandos *EUCOM* und *AFRICOM* zuständig.[1135] Luftwaffenkommandos wie *AFRICOM, EUCOM* und *CENTCOM*[1136] seien eine „Quelle für [...] Einsätze“, so *Bryant*.[1137]

1130) *Bryant*, Protokoll-Nr. 67 I, S. 75.

1131) *Bryant*, Protokoll-Nr. 67 I, S. 23.

1132) *Bryant*, Protokoll-Nr. 67 I, S. 73.

1133) Vgl. Zweiter Teil Feststellungen des Untersuchungsausschusses, Teil H, S. 95 ff.

1134) Vgl. Zweiter Teil Feststellungen des Untersuchungsausschusses, Teil H, S. 95 ff.

1135) Vgl. MAT A BMVg-3/1g, Bl. 70(VS-NfD); vgl. Zweiter Teil Feststellungen des Untersuchungsausschusses, Teil H, S. 95 ff.

1136) Regionalkommandos der US-Streitkräfte für Afrika (mit Ausnahme Ägyptens), Europa und Zentralkommando für Nahen Osten, Ostafrika und Zentralasien.

1137) *Bryant*, Protokoll-Nr. 67 I, S. 62.

Das DGS ist fester Bestandteil der über Ramstein gesteuerten Drohneneinsätze. Es sei

> „(…) eine Bodenstation, die beobachtet – – Die sind diejenigen, die den Video-Feed ansehen und verteilen“.[1138]

Die als „Screener“ bezeichneten Bildanalyst_innen im DGS seien für die Auswertung des Video-Feeds verantwortlich, also zum Beispiel für die optische Identifizierung von Zielpersonen.[1139] Das DGS in Ramstein nimmt als eines von weltweit insgesamt fünf solcher Stationen eine Kernrolle im Drohnenprogramm der USA ein.[1140]

In den dem Ausschuss zur Verfügung stehenden Quellen und der Aussage *Bryants* wird die Ausschließlichkeit der Rolle Ramsteins als Satellitenrelais deutlich.

Zwar soll derzeit auf dem NATO-Stützpunkt in Sigonella in Italien eine neue Relais-Station eingerichtet werden, jedoch gibt es weder offizielle Angaben dazu, noch konnten die dazu befragten Zeug_innen im Ausschuss Auskunft geben. Es ist daher davon auszugehen, dass Ramstein nach wie vor den US-Drohnenkrieg im Nahen Osten und in Afrika erst ermöglicht und daher nicht nur als eine, sondern als *die* Relais-Station fungiert.

b) Bundesregierung verschließt die Augen vor der zentralen Rolle Ramsteins für den US-Drohnenkrieg

Im Verhältnis zu der hohen Relevanz Ramsteins für die Durchführung von US-Drohnenangriffen in Afrika und dem Nahen Osten und der Implikation dessen für deutsche Bundesministerien konnte der Themenkomplex im Untersuchungsausschuss insbesondere aus offenkundig mangelndem Aufklärungsinteresse der Mehrheit nicht in der nötigen Tiefe untersucht werden, obwohl vor allem die Abgeordneten der Opposition in den Zeugenvernehmungen immer wieder auf Aufklärung der Fragen zu Ramstein und dem US-Drohnenkrieg drängten.

1138) *Bryant*, Protokoll-Nr. 67 I, S. 61.

1139) *Bryant*, Protokoll-Nr. 67 I, S. 33.

1140) *Bryant*, Protokoll-Nr. 67 I, S. 64; vgl. Zweiter Teil Feststellungen des Untersuchungsausschusses, Teil H, S. 7.

Dies lag vor allem an der mangelnden Bereitschaft der Bundesregierung, Informationen zu Ramstein zu beschaffen bzw. – soweit diese vorgelegen haben – weiterzugeben.

Seit der Veröffentlichung mehrerer Medienberichte mit Hinweisen zur Bedeutung der Air Force Base hatten sich Abgeordnete der Opposition immer wieder um Aufklärung durch die Bundesregierung bemüht. In zahlreichen parlamentarischen Anfragen baten sie die Bundesregierung um Auskunft oder eine Stellungnahme. Dabei sei es

> „von besonderem Interesse, welche Initiativen sie ergriffen hat, um die berichteten Verletzungen des Völkerrechts von deutschem Territorium aus entschieden zu unterbinden."[1141]

Die Bundesregierung ging in ihren Antworten mehrere Jahre nicht darauf ein, ob und wenn ja, welche Funktion Ramstein für US-Drohneneinsätze habe. Es wurde stets darauf verwiesen, die US-Streitkräfte hätten versichert, dass von amerikanischen Einrichtungen in Deutschland bewaffnete Drohneneinsätze weder geflogen noch befehligt würden und dass geltendes Recht eingehalten werde.[1142] Gegenteiliges war aber auch von Oppositionsseite nicht behauptet worden. Vielmehr war und ist die zentral zu klärende Frage, wie die Datenverarbeitung und -analyse in Ramstein vonstattengeht und welche Handlungen genau auf deutschem Boden im Kontext des US-Drohnenkrieges stattfinden.

aa) Kenntnis des Bundesministeriums der Verteidigung seit 2011

Dabei hatte das *BMVg* laut Aktenlage seit Ende 2011 Kenntnis von der in Ramstein geplanten Relaisstation: In einem Schreiben der US-Streitkräfte vom 18. November 2011 wurde über die beabsichtigte Errichtung einer „UAS SATCOM Relais Plattform

1141) Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion Bündnis 90/DIE GRÜNEN „Hinweise auf völkerrechtswidrige Praktiken der USA von deutschem Staatsgebiet aus und die diesbezüglichen Kenntnisse der Bundesregierung", Bundestagsdrucksache 18/237, S. 1. (Vorbemerkung der Fragesteller).

1142) Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion Bündnis 90/DIE GRÜNEN „Hinweise auf völkerrechtswidrige Praktiken der USA von deutschem Staatsgebiet aus und die diesbezüglichen Kenntnisse der Bundesregierung"; Bundestagsdrucksache 18/237, S. 10.

und Anlage“[1143] informiert und hatte dieser eigens zugestimmt.[1144] Es ist auch nicht möglich, dass sich das *BMVg* der Funktion der geplanten Relais gänzlich unbewusst war, da in dem Benachrichtigungsschreiben an das Ministerium eindeutig auf das Ziel des Bauvorhabens eingegangen wurde:

> „Mit Hilfe diese Maßnahme wird ein einzigartiges Kontrollzentrum für den Einsatz der Predator, Reaper und Global Hawk zur Unterstützung bei der […] Operation Iraqi Freedom (OIF) und Operation Enduring Freedom (OEF) geschaffen.“[1145]

Predator, Reaper und Global Hawk sind und waren bekanntermaßen Kampfdrohnen, die die US-Armee seit Beginn des Drohnenprogramms für gezielte Tötungen einsetzt.[1146]

Die Kenntnis von der Schaffung eines Kontrollzentrums für Kampfdrohneneinsätze auf deutschem Boden hätte die Bundesregierung zu sehr viel größeren Bemühungen um genaue Informationen von US-Seite bewegen müssen, als jene zurückhaltenden Konsultationen und Nachfragen, die sie nach den eigenen Angaben auf parlamentarische Anfragen unternommen haben will.

bb) Mangelhaftes Aufklärungsbemühen

Zeugenaussagen von Regierungsmitgliedern im Untersuchungsausschuss zu diesem Thema erwecken den Eindruck von Unkenntnis und mangelndem Aufklärungsbemühen. So versicherte beispielsweise *Dr. Frank-Walter Steinmeier* in seiner Vernehmung:

> „Wir sind unablässig dabei, Aufklärung zu erreichen. Wir haben dazu auf verschiedenen Ebenen – das habe ich alles in früheren Antworten

---

1143) Benachrichtigungsschreiben der US-Streitkräfte vom 18. November 2011, MAT A BMVg-3/5f_1, Bl. 296.

1144) Vgl. Abschlussbericht 1. Untersuchungsausschuss, Zweiter Teil: Feststellungen des Untersuchungsausschusses, Teil H, S. 14: „Am 15. Dezember 2011 erklärte das BMVg, gegen das von den US-Streitkräften vorgeschlagene Vorhaben im Truppenbauverfahren keine Bedenken zu haben.“

1145) Benachrichtigungsschreiben der US-Streitkräfte vom 18. November 2011, MAT A BMVg-3/5f_1, Bl. 286.

1146) Einführend *Grégoire Chamayou* (2012), Ferngesteuerte Gewalt: Eine Theorie der Drohne, Passagen Verlag, S. 37 ff.; *Kai Biermann/Thomas Wiegold* (2015), Drohnen. Chancen und Gefahren einer neuen Technik, Chr. Links Verlag Berlin, S. 42 ff.

> schon mal ausgeführt – mit den amerikanischen Partnern im Gespräch. Wir haben bisher keine Aufklärung darüber, welche technische Rolle Ramstein als Relaisstation für Drohnenangriffe zum Beispiel in Afrika bedeutet. Ob das alternativlos ist, ob das eine Relaisstation ist, die in einer Kette von anderen Relaisstationen steht, das ist bisher nicht ausreichend geklärt.“[1147]

Im Ausschuss und in der Öffentlichkeit wurde u.a. von der Opposition der Vorwurf erhoben, die Bundesregierung verschließe die Augen und nehme ihre verfassungsrechtliche und völkerrechtliche Verantwortung bezüglich der Relaisstation in Ramstein nicht wahr. Die Bewertung der Koalitionsmehrheit hält dies für aus der Luft gegriffen.[1148] Angesichts der geschilderten Insiderkenntnisse des Zeugen *Bryant* und der Ankündigung für die Errichtung der Relaistation trifft dies wohl eher für die ausweichenden Reaktionen und Antworten der Bundesregierung zu.

In Reaktion auf eine weitere Kleine Anfrage der Fraktion DIE LINKE im Oktober 2014 teilte die Bundesregierung mit, sie habe

> „der amerikanischen Botschaft in Berlin im April 2014 einen Katalog mit Fragen über eine mögliche Beteiligung von deutschen Standorten der US-Streitkräfte an bewaffneten Einsätzen unbemannter Luftfahrzeuge übermittelt.“[1149]

Die Beantwortung dieses Fragenkatalogs zu Ramstein und AFRICOM sollte laut Antwort des Auswärtigen Amts auf Nachfrage im Juli 2014 nur noch wenige Woche dauern.[1150]

1147) *Dr. Steinmeier*, Protokoll-Nr. 91 I, S. 77.

1148) Mehrheitsbewertung, S. 109

1149) Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion DIE LINKE. „Die Rolle des United Staates Africa Commands und der US-Militärbasis in Ramstein für US-Drohnenangriffe“ Bundestagsdrucksache 18/2794, S. 2.

1150) Antwort Staatsministerin *Dr. Maria Böhme* (AA) vom 2. Juli 2014 auf die Frage des Abg. *Andrej Hunko,* Plenarprotokoll 18/45, S. 4038.

Tatsächlich steht eine abschließende Antwort bis zum heutigen Tage aus. Abgeordnete werden auch drei Jahre nach Entsendung des Fragekatalogs auf später vertröstet.[1151]

Auf wiederholte Nachfragen des Abgeordneten *Andrej Hunko* (DIE LINKE.) erwiderte die Bundesregierung:

> „Der Beauftragte für Sicherheitspolitik im Auswärtigen Amt war außerdem im September 2015 in Ramstein und hat dort Gespräche geführt. Eine abschließende Klärung konnte bislang aber nicht erzielt werden. Die Bundesregierung bleibt in dieser Frage im vertraulichen Dialog mit der amerikanischen Regierung.“[1152]

Am 30. November 2016 – mehr als zwei Jahre nach Entsendung des Fragenkataloges – bestätigte die Bundesregierung in einer parlamentarischen Fragestunde durch *Michael Roth*, Staatsminister im Auswärtigen Amt, erstmals öffentlich die Funktion der Air Base Ramstein als Relais-Station für Drohneneinsätze.[1153]

Die US-Botschaft habe in einem Gespräch am 26. August 2016 mitgeteilt,

> „dass die globalen Kommunikationswege der USA zur Unterstützung unbemannter Luftfahrzeuge, Fernmeldepräsenzpunkte auch in Deutschland einschlössen, von denen aus die Signale weitergeleitet würden. Einsätze unbemannter Luftfahrzeuge würden von verschiedenen Standorten aus geflogen, unter Nutzung diverser Fernmelderelaisschaltungen, von denen einige auch in Ramstein laufen würden.“[1154]

1151) Antwort Staatsministerin *Dr. Maria Böhme* (AA) vom 17. Mai 2017 auf die Frage des Abg. *Niema Movassat*, Plenarprotokoll 18/233, S. 23573.

1152) Antwort des Staatsministers *Michael Roth* (AA) vom 22. Juni 2016 auf die Frage des Abg. *Andrej Hunko*, Plenarprotokoll 18/178, S. 17564.

1153) Antwort des Staatsministers *Michael Roth* (AA) vom 30. November 2016 auf die Frage des Abg. *Andrej Hunko*, Plenarprotokoll 18/205, S. 20452.

1154) Antwort des Staatsministers *Michael Roth* (AA) vom 30. November 2016 auf die Frage des Abg. Andrej Hunko, Plenarprotokoll 18/205, S. 20452.

> „Außerdem teilte sie mit, dass im Jahr 2015 in Ramstein eine Vorrichtung zur Verbesserung der bereits zuvor vorhandenen Fernmeldeausstattung fertiggestellt worden sei, und sie hat uns darüber informiert, dass Ramstein eine Reihe weiterer Aufgaben unterstütze, darunter die Planung, Überwachung, Auswertung von zugewiesenen Luftoperationen. In Reaktion auf diese neuen Informationen haben wir hochrangige Gespräche in Washington Mitte September geführt, wiederum über unseren Politischen Direktor, und wir werden dazu selbstverständlich auch weiterhin mit der amerikanischen Seite in Kontakt bleiben.“[1155]

Die Brisanz dieser ersten öffentlichen Erklärung der Bundesregierung, um die tatsächliche Funktion Ramsteins als Relais zu wissen, spielte der Staatsminister herunter, indem er darauf hinwies, die Bundesregierung habe sich bereits im September gegenüber den Obleuten des Auswärtigen Ausschusses zu diesem Thema geäußert und vom diesbezüglichen Gespräch mit der US-Regierung berichtet. Im Bundestagsplenum oder dem mit dem Thema primär befassten Untersuchungsausschuss gegenüber waren diese Informationen von der Bundesregierung zu keinem Zeitpunkt freiwillig offeriert und berichtet worden. Nur auf ausdrückliche Nachfrage erfuhren so die Fachpolitiker_innen und Abgeordneten des Untersuchungsausschusses von dieser neuen Entwicklung.[1156]

4. Datenübermittlungen deutscher Behörden an Dienste der Five-Eyes-Staaten und deren Nutzbarkeit für tödliche US-Drohneneinsätze

Nicht nur die Hauptstelle für Befragungswesen[1157] und andere BND-Stellen[1158] gaben personenbezogene Daten an Dienste der Five Eyes weiter, sondern offenbar auch das Bundesamt für Verfassungsschutz.

1155) Antwort des Staatsministers *Michael Roth* (AA) vom 30. November 2016 auf die Frage des Abg. Andrej Hunko, Plenarprotokoll 18/205, S. 20452.

1156) Beratungsprotokoll-Nr. 123, 125 und 127.

1157) Vgl. Kap. XI. – Hauptstelle für Befragungswesen

1158) Vgl. Kap. V.8. – Datenübermittlungen des BND an die NSA aus Bad Aibling

Für den Untersuchungsausschuss war in diesem Zusammenhang die Diskussion über die Lokalisierungsmöglichkeiten durch Mobilfunkdaten relevant, weil es zur gängigen Praxis der deutschen Nachrichtendienste gehört, Daten – auch Mobilfunkdaten – an AND, insbesondere US-Dienste wie NSA, CIA und FBI weiterzuleiten.[1159] Deshalb stand die Frage im Raum, ob diese weitergeleiteten Daten mitursächlich für US-Drohnenangriffe und gezielte Tötungen von Menschen gewesen sein können.

Im BfV wurde die Zusammenarbeit mit AND über die Abteilung 1 koordiniert und fand dann in den jeweiligen Fachbereichen statt.[1160] Besonders eng war die Kooperation in der Abteilung 6, zuständig für Islamismus und islamischen Terrorismus. Es gab laut Zeugenaussagen auch einen Verbindungsbeamten der NSA, der regelmäßig in die BfV-Liegenschaft in Berlin-Treptow kam.[1161]

Die Weitergabe von Mobilfunkdaten wurde dabei lange Zeit unhinterfragt praktiziert, die technische Möglichkeit der Geolokalisierung aufgrund von Mobilfunkdaten ignoriert oder geleugnet. Tatsächlich waren die verschiedenen Möglichkeiten der geografischen Zuordnung von Mobilfunkdaten den deutschen Behörden lange bekannt.

a) Technische Lokalisierung von Mobilfunkgeräten

Alle zur Problematik der technischen Lokalisierung von Mobilfunkgeräten (MFG) vernommenen Zeugen aus dem BfV, dem BMI, dem BND und dem Bundeskanzleramt sagten in unterschiedlicher Form aus, dass sich Mobilfunkdaten mit Ausnahme von GPS nicht oder nicht hinreichend genau zur Ortung nutzen ließen. Auch die Bundesregierung versicherte in Auskünften, Mobilfunknummern eigneten sich nicht zu einer zielgenauen Lokalisierung.[1162] Diese Bezeugungen werden durch die gutachterliche Stellungnahme des Sachverständigen *Prof. Dr. Hannes Federrath* vom 19. September 2016 widerlegt. Demnach sind und waren während des Untersuchungszeitraums folgende Daten in Mobilfunknetzen geeignet, MFG weltweit zu lokalisieren:

1159) *Berfuß*, Protokoll-Nr. 96 I, S. 51.

1160) *Treuenfels*, Protokoll-Nr. 97 I, S. 57.

1161) *Berfuß*, Protokoll-Nr. 96 I, S. 16.

1162) Siehe Zweiter Teil: Feststellungen des Untersuchungsausschuss, Kap. H. I. 1. h) dd).

> „öffentliche und netzinterne Rufnummern eines mobilen Teilnehmers:
>
> – Mobile Subscriber Integrated Services Digital Network Number (MSISDN),
>
> – International Mobile Subscriber Identity (IMSI),
>
> Gerätekennungen eines mobilen Teilnehmers:
>
> – International Mobile Equipment Identity (IMEI),
>
> – Electronic Serial Number (ESN),
>
> – Mobile Equipment Identifier (MEID) sowie
>
> ggf. weitere personenbezogene bzw. gerätespezifische Identifizierungsmerkmale wie beispielsweise die MAC-Adresse, welche eine Zuordnung von Datenverkehr zu einem Gerät bzw. einer Person ermöglichen.“[1163]

Weiter führt er aus:

> „Eine Telefonnummer (typischerweise die MSISDN) bzw. die netzinternen Rufnummern und Gerätekennungen (z.B. die IMEI und IMSI) sind unter günstigen atmosphärischen Bedingungen als einzige technische Daten ausreichend, um eine Fernlenkwaffe mit einem tödlichen Radius von 5 m mit hinreichender Treffergenauigkeit für eine gezielte Tötung einsetzen zu können. Die Zielführung mit Laser auf Basis einer ggf. zuvor durchgeführten Lokalisierung mit den nachfolgend beschriebenen Verfahren dürfte jedoch das übliche Verfahren der Fernlenkung sein.“[1164]

Die gutachterliche Stellungnahme zeigt darüber hinaus eindringlich die technischen Möglichkeiten auf, die zur Identifizierung und Lokalisierung von MFG des Massen-

1163) Schriftliches Gutachten des Sachverständigen Prof. *Dr. Federrath*, MAT A SV 14/2, S. 6.

1164) Schriftliches Gutachten des Sachverständigen Prof. *Dr. Federrath*, MAT A SV 14/2, S. 6.

marktes in den Mobilfunknetzen GSM, UMTS und LTE bestehen. Hierzu zählen insbesondere die Zuordnung einer Mobilfunknummer (MSISDN) zur entsprechenden netzinternen Kennung IMSI über das standardisierte Protokoll Signaling System No.7 (SS7) zur Abfrage und Übermittlung von mobilfunkinternen Daten, die Lokalisierung einer aktuellen Funkzelle, in die ein MFG eingebucht ist, durch Zugriff auf das SS7-Protokoll, die Positionsbestimmung mittels Laufzeitpeilung durch stationäre Mobilfunkbasisstationen und durch GPS sowie die Lokalisierung durch IMSI-Catcher. Letztere erlauben es, eine reguläre Basisstation eines Mobilfunknetzes zu simulieren, in die sich alle im Einzugsbereich des Catchers erreichbaren MFG einbuchen, und ein entsprechendes MFG durch das Auslesen der IMSI und der IMEI zu lokalisieren.

Die Angriffsmöglichkeit mittels eines IMSI-Catchers entspricht der, die der Zeuge *Bryant* unter dem Stichwort „GILGAMESH“ für entsprechende an US-Drohnen montierte Geräte beschrieb.[1165] Die Ortung von Zielpersonen mithilfe des GILGAMESH-Pods erläuterte *Bryant* wie folgt:

> „Der Gilgamesh-Pod funktionierte sozusagen als eigener Funkmast […] Nun, das Mobiltelefon wählt immer das stärkste Signal aus, und das stärkste Signal ist immer da, der Funkmast. Was wir also machen, ist, wir pingen diese Funkmasten für den Zugang an – zum Beispiel die Handys, die angerufen werden, oder so etwas –, und sobald unser Pod erkennt, dass das Handy benutzt wird, versucht er auch, dieses Handy vom Funkmast auf unseren zu ziehen und dann das Signal zwischen dem Funkmast und uns zu triangulieren, um so die Zielperson zu orten.“[1166]

Durch die Bewegungen der Drohne am Himmel kann festgestellt werden, ob die Verbindung stärker oder schwächer wird und damit der genaue Standort des Geräts ermittelt werden. In der gutachterlichen Stellungnahme des Sachverständigen *Federrath* wird die autonome Lokalisierung von MFG des Massenmarktes durch eine Drohne in

1165) *Bryant*, Protokoll-Nr. 67 I – Teil 1, S. 38, 51 f. u. 102.

1166) *Bryant*, Protokoll-Nr. 67 I – Teil 1, S. 51 f.

den einzelnen Schritten beschrieben. Bezogen auf die eingangs genannte Treffergenauigkeit heißt es dort an anderer Stelle:

> „Somit ergibt sich unter günstigen atmosphärischen und geographischen Bedingungen die Möglichkeit, eine Fernlenkwaffe mit einem tödlichen Radius von 5 m mit hinreichender Treffergenauigkeit für eine gezielte Tötung einsetzen zu können.
>
> Fernlenkwaffen wie die Hellfire-Raketen sollen mit einem 9 kg schweren Gefechtskopf einen bis zu 20 m großen tödlichen Radius haben. Üblicherweise werden diese Systeme mit Laserunterstützung ferngelenkt.“
>
> „Die konkrete Ausgestaltung des Mobilfunkverkehrs in den Ländern Afghanistan, Pakistan, Jemen und Somalia während des Untersuchungszeitraumes ist für die hier beschriebene Lokalisierung mittels IMSI-Catcher bedeutungslos, da das Lokalisierungsverfahren autonom arbeitet, d.h. nicht auf die Infrastruktur des Mobilfunknetzes angewiesen ist.“[1167]

Der Ausschuss hat abschließend feststellen können, dass eine Zielerfassung allein auf der Basis von Mobilfunkdaten möglich ist und übermittelte Mobilfunkdaten jedenfalls eine entscheidende Rolle bei der Zielauswahl und -erfassung für tödliche Drohneneinsätze gespielt haben.

b) Datenübermittlung erfolgte wider besseren Wissens

Die Aussagen der Bundesregierung und im Rahmen des Untersuchungsausschusses jene von Zeug_innen des BfV, BND und BMI, Mobilfunkdaten mit Ausnahme von GPS eigneten sich nicht zur zielgenauen Lokalisierung von MFG sind unzutreffend. Die wiederholte Behauptung, von der technischen Möglichkeit der Ortung durch MFG habe

1167) Schriftliches Gutachten des Sachverständigen *Prof. Dr. Federrath*, MAT A SV 14/2, S. 17.

man „überhaupt keine Kenntnis gehabt“[1168] ist angesichts der Tatsache, dass deutsche Dienste selbst von Lokalisierungsmethoden wie IMSI-Catchern Gebrauch gemacht haben, unglaubwürdig.

aa) Einsatz von IMSI-Catchern durch deutsche Dienste

In Deutschland wurden IMSI-Catcher Mitte der 1990er Jahre von der Firma Rohde & Schwarz entwickelt.[1169] Die Rechtsgrundlage für deren Einsatz durch die nachgeordneten Bundesbehörden BfV und BND wurde mit dem Terrorismusbekämpfungsgesetz 2002, geändert mit dem Terrorismusbekämpfungsergänzungsgesetz 2007, geschaffen.[1170] Spätestens seitdem besteht dort die technische Expertise über den Einsatz von IMSI-Catchern und deren Funktionsweise und wird über die Anzahl der IMSI-Catcher-Einsätze durch BfV und BND in den vom Parlamentarischen Kontrollgremium herausgegebenen Jahresberichten über Maßnahmen nach dem Terrorismusbekämpfungsgesetz berichtet. Im Evaluationsbericht der Bundesregierung vom 17. Juni 2005 zum Terrorismusbekämpfungsgesetz von 2002, das den Einsatz „technische[r] Mittel zur Ermittlung des Standortes eines aktiv geschalteten Mobilfunkendgerätes oder zur Ermittlung der Geräte- oder Kartennummer“[1171] durch den Verfassungsschutz oder den BND erlaubte, heißt es:

> „Mit Artikel 1 Nr. 4 Buchstabe c Terrorismusbekämpfungsgesetz ist in dem neuen § 9 Abs. 4 BVerfSchG eine spezielle Befugnis zum Einsatz des sogenannten ‚IMSI-Catchers‘ geschaffen worden. Der Einsatz

1168) *Fromm*, Protokoll-Nr. 102 I, S. 31.

1169) *Dirk Fox*: Der IMSI-Catcher. In: Datenschutz und Datensicherheit 26 (2002), 4, S. 212-215.

1170) Gesetz zur Bekämpfung des internationalen Terrorismus vom 9. Januar 2002, TBG, BGBl. I S. 361; Gesetz zur Ergänzung des Terrorismusbekämpfungsgesetzes vom 5. Januar 2007, TBEG, BGBl. I S. 2.

1171) Vgl. § 9 Abs. 4 BVerfSchG: Besondere Formen der Datenerfassung, zuletzt geändert am 5. Januar 2007.

> des IMSI-Catchers dient der Ermittlung der Geräte- und Kartennummer von Mobiltelefonen […] und auf dieser Basis auch zur Lokalisierung des Standortes des Gerätes.“[1172]

In dem dazugehörigen Hinweispapier des BMI zu „Fakten zur Evaluierung des Terrorismusbekämpfungsgesetzes“ ist angegeben, dass das BfV bis dahin für 21 Personen den Einsatz von IMSI-Catchern angeordnet hat.[1173]

bb) Deutsche Behörden verschlossen die Augen

Innerhalb der Bundesregierung und ihrer Behörden wurde die Eignung von Daten wie Mobilfunknummern für die Zielerfassung entgegen den tatsächlichen technischen Bedingungen in Abrede gestellt. Einschätzungen wie die des Zeugen *Stefan Kaller*, Leiter der Abteilung Öffentliche Sicherheit im BMI, der die Durchführung von US-Militäreinsätzen allein aufgrund der Ortung eines Handys für nicht plausibel und „denklogisch und auch von der Praxis her ausgeschlossen“[1174] erklärte, folgen dabei offenbar der Logik, dass nicht sein kann, was nicht sein darf.

Auch der Zeuge *Dettmer*, ab 2007 imBfV tätig, erklärte dazu:

> „Wenn ich mich recht erinnere, war die Position, die im Hause vertreten wurde, dass die Übermittlung, also die Handydaten alleine, nicht für eine zielgenaue Ortung im Zielgebiet reichen.“[1175]

1172) Bericht der Bundesregierung zu Auswirkungen des Terrorismusbekämpfungsgesetzes, S. 28, https://www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/Sicherheit/Terrorismus/Bericht_BReg_Auswirkung_Terrorismusbekaempfungsgesetz.pdf?__blob=publicationFile (abgerufen ab 5. Juni 2016).

1173) Hinweispapier des BMI: „Fakten zur Evaluierung des Terrorismusbekämpfungsgesetzes“ vom 17. Juni 2005, S. 3, http://www.bmi.bund.de/cae/servlet/contentblob/132848/publicationFile/9102/ (6. Juni 2017).

1174) *Kaller*, Protokoll-Nr. 106 I, S. 33.

1175) *Dettmer*, Protokoll-Nr. 98 I, S. 120.

Nach dem Verständnis der dazu befragten Zeug_innen des BfV eigneten sich GPS-Koordinaten zur „unmittelbare[n] Lokalisierung“[1176] von Personen, sonstige Mobilfunkdaten wie Handynummern jedoch seien „nur sehr grob geeignet“.[1177] Der ehemalige BfV-Präsident *Fromm* sagte im Ausschuss aus:

> „Ich hatte solche Informationen über solche technischen Kombinationen, IMSI-Catcher usw., zur damaligen Zeit nicht, […] – und ganz offensichtlich, ganz offensichtlich auch nicht das Ministerium.“[1178]

Dabei war er von 2000 bis 2012 Verfassungsschutzpräsident gewesen, also während der Schaffung der Rechtsgrundlage, die erlauben sollte, was bis dahin zwar technisch möglich, aber rechtlich noch nicht zulässig war, und in der Folge wiederholt zum Einsatz kam: Die Lokalisierung von Mobilgeräten durch den Einsatz von IMSI-Catchern.

Der BND hatte ganz klare Vorstellung über die Verwendungsmöglichkeiten dieser Daten. So heißt es in einer E-Mail von Januar 2012:

> „[redacted]“[1179]

Dass deutsche Behörden wie das BMI oder BfV und BND angeblich keine Kenntnis davon hatten und teilweise bis heute daran festhalten, dass Mobilfunkdaten nicht zur Ortung geeignet seien, ist angesichts dessen eine bewusste Irreführung von Parlament und Öffentlichkeit. Sollte diese Haltung auch heute noch der geheimdienstlichen Übermittlungspraxis personenbeziehbarer Daten an AND zugrunde liegen, wäre das mindestens grob fahrlässig.

1176) *Isselburg*, Protokoll-Nr. 100, S. 78.

1177) *Treuenfels*, Protokoll-Nr. 94 II – Auszug offen, S. 12, auch *Berfuß*, Protokoll-Nr. 96 I, S. 43; *Fromm*, Protokoll-Nr. 102 I, S. 28..

1178) *Fromm*, Protokoll-Nr. 102 I, S. 35.

1179) MAT A BND-49/1, Bl. 25 (VS-NfD)

c) Der Romann-Erlass

Im Herbst 2010 sollte eine Liste mit personenbezogenen Daten – Personaldaten, Passdaten, den Personen zugeordnete Kommunikationsmittel – an AND übermittelt werden.[1180] Am 15. Oktober 2010 bat das BfV das zuständige Referat im BMI um eine Genehmigung zur Übermittlung dieser Liste.[1181] Einige Wochen später teilte *Dr. Romann*, der zuständige Referatsleiter im BMI, dem damaligen BfV-Präsidenten *Heinz Fromm* mit, die Übersendung der Liste sei genehmigt, soweit diese keine zur Ortung geeigneten Daten enthalte.[1182] Als daraufhin das BfV um eine Genehmigung für die Weiterleitung zweier weiterer Listen an AND bat, erließ *Dr. Romann* folgende Weisung, im Ausschuss auch als „Romann-Erlass" bezeichnet:

> „BMI stimmt der Übermittlung der Daten an die gennannten Länder grundsätzlich zu. Vor einer Übermittlung ist sicherzustellen, dass die Listen keine Daten enthalten, die unmittelbar für eine geografische Ortung in der in Rede stehenden Region verwendet werden können."[1183]

Wie in den Aussagen der BfV-Zeug_innen deutlich wird, waren Mobilfunkdaten nach deren Verständnis von dieser Formulierung nicht umfasst. Diese Auffassung bestätigte auch der Zeuge *Dr. Romann*:

> „[…] zulässig nach dem Erlass ist wie vorher und nachher die Übermittlung von Mobilfunkdaten."[1184]

Spätestens nachdem der ehemalige NSA- und CIA-Chef *Michael Hayden* im April 2014 bei einer Podiumsdiskussion der *Johns Hopkins* University erklärt hatte: „Wir töten auf der Basis von Metadaten", müssen die deutschen Sicherheitsbehörden davon

1180) *Isselburg*, Protokoll-Nr. 100 I, S. 75 f.

1181) *Dr. Romann*, Protokoll-Nr. 100 I, S. 125.

1182) *Dr. Romann*, Protokoll-Nr. 100 I, S. 125.

1183) MAT A BMI-21/1, Bl. 1. (VS-NfD)

1184) *Dr. Romann*, Protokoll-Nr. 100 I, S. 130.

ausgehen, dass die von ihnen übermittelten Daten regelmäßig für die Planung und ggf. Durchführung tödlicher Drohneneinsätze verwendet werden.[1185] ,

Diese Praxis hätte jedoch vor dem Hintergrund, dass eine Lokalisierung mithilfe von Handynummern nicht auszuschließen ist, vom BMI unmissverständlich untersagt werden müssen.

Die Verantwortung für die Weitergabe der in Frage stehenden BfV-Daten an AND liegt bei der Fachaufsicht des Bundesinnenministeriums. Das von *Dr. Romann* geleitete Referat hätte bei Kenntnis einer solchen Liste die betreffenden Daten, zum Beispiel Handynummern, für eine Weiterleitung an AND sperren müssen, anstatt nur einen Erlass „rein deklaratorischer Natur“[1186] auszusprechen.[1187]

d) Fälle mit Deutschlandbezug

Der Romann-Erlass war eine Reaktion auf die öffentliche Diskussion, die durch den Tod der deutschen Staatsangehörigen *Bünyamin Erdogan* und *Shahab Dashti Sineh Sar* durch einen Drohnenangriff am 4. Oktober 2010 nahe der pakistanischen Stadt Mir Ali ausgelöst wurde.[1188]

Insgesamt sind sieben Fälle von Personen bekannt, deren Daten das BfV an US-Geheimdienste weitergeleitet hatte und die nach ihrer Ausreise ins afghanisch-pakistanische Grenzgebiet durch Drohnenangriffe getötet wurden.[1189]

Zwar wurde versichert

> „[…] selbstverständlich will und wollte das BfV kein Teil des Drohnenkriegs der Amerikaner sein“[1190],

1185) *Michael Hayden* auf dem *Johns Hopkins Foreign Affairs Symposium* am 1. April 2014 zum Thema „The Price of Privacy: Re-Evaluating the NSA“, vgl. 00:17:53, https://www.youtube.com/watch?v=kV2HDM86XgI (abgerufen am 4. Juni 2017).

1186) Dr. Romann, Protokoll-Nr. 100 I, S. 141.

1187) *Dr. Romann*, Protokoll-Nr. 100 I, S. 125.

1188) *Dr. Romann*, Protokoll-Nr. 100 I, S. 141.

1189) Vgl. *Isselburg*, Protokoll-Nr. 100 I, S. 76.

1190) *Isselburg*, Protokoll-Nr. 100 I, S. 88.

die Praxis der Weitergabe von Mobilfunkdaten wurde jedoch zu keinem Zeitpunkt eingestellt. Auch im Falle der Drohnenopfer *Bünyamin Erdogan* und *Shahab Dashti Sineh Sar* waren Daten, darunter Mobilfunknummern, vom BfV an einen US-amerikanischen Geheimdienst übermittelt worden, wie Zeugenaussagen bestätigten.[1191]

e) Verwendung von Daten aus Befragungen im Militärgefängnis Bagram für gezielte Tötungen?

Ebenfalls für Diskussionen sorgte eine im engen zeitlichen Zusammenhang mit dem tödlichen Drohneneinsatz in Mir Ali stehende Befragung von deutschen und US-amerikanischen Geheimdiensten im US-Militärgefängnis auf der Air Base Bagram in Afghanistan. Zwar wurde dieser Themenkomplex von der Bundesregierung wiederholt für nicht untersuchungsgegenständlich erklärt, die Oppositionen haben aber erhebliche Zweifel an dieser Sichtweise..[1192]

Am 3. Oktober 2010, also einen Tag vor dem Drohnenangriff in Mir Ali, wurde der deutsche Staatsangehörige *Ahmad Sidiqi* im US-Militärgefängnis in Bagram von jeweils zwei Beamten des *BND* und des *BfV* befragt.[1193] Laut Aussage des Zeugen *Isselburg,* der selbst bei der Befragung anwesend war, waren auch US-Militärangehörige vor Ort.[1194]

Ahmad Sidiqi war wie auch *Bünyamin Erdogan* und *S. Dashti Sineh Sar* Teil der Hamburger Gruppe von mutmaßlichen Islamisten, die im März 2009 gemeinsam ins afghanisch-pakistanische Grenzgebiet ausgereist waren. Er kannte die beiden am nächsten Tag durch den Drohnenangriff Getöteten also persönlich. Laut Presseberichten hatte *Sidiqi* den Befragern

> „bereitwillig Auskunft gegeben, vor allem über die deutsche Islamisten-Szene“.[1195]

1191) *Fromm*, Protokoll-Nr. 102 I, S. 7f.; *Dr. Romann*, Protokoll-Nr. 100 I, S. 145.

1192) Vgl. hierzu Kapitel III.2.b)bb) Gefangenenbefragung im US-Militärgefängnis in Bagram

1193) Vgl. *Isselburg*, Protokoll-Nr. 100 II – Auszug offen, S. 8 f.

1194) *Isselburg*, Protokoll-Nr. 100 II – Auszug offen, S. 8.

1195) Frankfurter Allgemeine Zeitung vom 11. Oktober 2010 – „BND verhört deutschen Al-Qaida-Anhänger“.

Die dazu befragten Zeugen des BfV sahen keinen Zusammenhang zwischen der Befragung von *Ahmad Sidiqi* und dem Drohnenangriff am nächsten Tag.[1196] Ob S*idiqi* Informationen zu seinen am nächsten Tag getöteten Bekannten preisgegeben hatte und ob diese gegebenenfalls als Kriterium für den Drohneneinsatz verwendet wurden, konnte nicht geklärt werden. Höchst problematisch war die Befragung durch deutsche Geheimdienste aber schon allein angesichts der Haftbedingungen in Bagram. In einem späteren Gerichtsverfahren gegen *Sidiqi* wurde von dessen Haft im Militärgefängnis berichtet: Diese habe er unter schweren hygienischen Mängeln, Dauerüberwachung und permanenter Helligkeit oder Dunkelheit verbracht.[1197]

Das Gefängnis in Bagram war in der Vergangenheit durch Foltermethoden bekannt geworden. So veröffentlichte die *New York Times* auf Grundlage eines Untersuchungsberichts des US-Militärs mehrere Informationen zu Folteropfern in Bagram, wie den Fall zweier afghanischer Inhaftierter, die von Soldat_innen zu Tode geschlagen wurden.[1198]

Dass *Sidiqi* an einem solchen Ort von deutschen Diensten befragt wurde, ist ein Skandal. In einem Dokument zum „Verfahren für künftige Befragungen von im Ausland – durch dortige Sicherheitskräfte – inhaftierte Personen durch Mitarbeiter deutscher Nachrichtendienste“ ist ausdrücklich vermerkt, dass

> „[e]ine Befragung unterbleibt wenn im Einzelfall konkrete Anhaltspunkte bestehen, dass der Betroffene im Aufenthaltsland der Folter unterworfen wird.“[1199]

Auch wird angewiesen:

1196) Vgl. *Fromm*, Protokoll-Nr. 102 I, S. 55; *Isselburg*, Protokoll Nr. 100 II – Auszug offen, S. 8.

1197) SWR-Terrorismus Blog vom 22. Mai 2012 – „Sechs Jahre Haft & harte Kritik an der CIA“, http://www.swr.de/blog/terrorismus/2012/0+5/22/6-jahre-haft-harte-kritik-an-der-cia/ (abgerufen am 07. Juni 2017).

1198) New York Times vom 20. Mai 2005: In U.S. Report, Brutal Details of 2 Afghan Inmates' Deaths, http://www.nytimes.com/2005/05/20/world/asia/in-us-report-brutal-details-of-2-afghan-inmates-deaths.html (abgerufen am 15. Juni 2017).

1199) Vgl. Verfügung des Bundeskanzleramtes vom 6.03.2006: Verfahren für künftige Befragungen von im Ausland durch dortige Sicherheitskräfte inhaftierten Personen durch Mitarbeiter deutscher Nachrichtendienste, Nr. 92 der beigefügten Dokumente für den Abschlussbericht des 1. Untersuchungsausschusses der 16. Wahlperiode (BND-Untersuchungsausschuss, Bundestagsdrucksache 16/13400.

> „Freiwilligkeit und das ausdrückliche Einverständnis des jeweiligen Betroffenen sind unverzichtbare Voraussetzungen."[1200]

Da die Vernehmung *Sidiqis* in Bagram durch BND und BfV stets für nicht untersuchungsgegenständlich erklärt wurde, bleibt der Verdacht einer unfreiwilligen und rechtswidrigen Befragung im Raum stehen.

f) Untauglichkeit des „Disclaimers" bei Datenübermittlungen

Die Verwendung der an AND weitergegebenen Daten sollte durch einen schriftlichen Verweis, auch „Disclaimer"[1201] genannt, beschränkt werden. Wie auch bei Datenübermittlungen des BND an AND[1202] fügte auch das BfV in die übermittelten Dokumente einen Standardtext ein, der darauf verwies, „dass die Daten nur zu dem Zweck verwendet werden dürfen, zu dem sie übermittelt wurden."[1203] Dabei handelte es sich um „deutsche nachrichtendienstliche Zwecke".[1204] Auf die Einhaltung dieses Verweises durch die Partnerdienste wurde lediglich vertraut.[1205]

Gleichzeitig sagte *Fromm* bezüglich der möglichen Nutzung übermittelter Mobilfunkdaten für eine genaue Lokalisierung und Zielerfassung aus:

> „Es ist natürlich denkbar, dass Informationen, die von uns geliefert wurden, Teil einer Gesamtinformation werden, die dann geeignet ist, solche einen gezielten Angriff durchzuführen."[1206]

1200) Vgl. Verfügung des Bundeskanzleramtes vom 6.03.2006: Verfahren für künftige Befragungen von im Ausland durch dortige Sicherheitskräfte inhaftierten Personen durch Mitarbeiter deutscher Nachrichtendienste, Nr. 92 der beigefügten Dokumente für den Abschlussbericht des 1. Untersuchungsausschusses der 16. Wahlperiode (BND-Untersuchungsausschuss, Bundestagsdrucksache 16/13400.

1201) Engl. für Ausschlussklausel.

1202) Vgl. dazu Kapitel V. 8. b) bb) Unklarer Zweck

1203) *Isselburg*, Protokoll-Nr. 100 I, S. 83.

1204) *Isselburg*, Protokoll-Nr. 100 I, S. 83.

1205) Vgl. *Isselburg*, Protokoll-Nr. 100 I, S. 84; Dettmer, Protokoll-Nr. 98 I, S. 121.

1206) *Fromm*, Protokoll-Nr. 102 I, S. 28.

Dass diese Daten entsprechend genutzt werden konnte, war den deutschen Behörden bekannt.[1207]

g) Identifizierung von Zielpersonen für US-Drohnenangriffe durch Metadaten und „Skynet“

Vor dem Hintergrund der Anfang April 2014 getätigten Aussage des ehemaligen NSA- und CIA-Direktors *Michael Hayden*: „We kill people based on metadata“,[1208] kann eine weitere Form der Nutzung von Metadaten im US-Drohnenkrieg nicht ausgeschlossen werden.

Nähere Einzelheiten zum NSA-Programm Skynet veröffentlichte im Mai 2015 das Online-Magazin *The Intercept*.[1209] Das Programm dient der Identifizierung von Zielpersonen für US-Drohnen im Anti-Terror-Krieg und nutzt Big-Data-Analysen auf Basis von maschinellem Lernen zur automatischen Musteridentifikation.

Das bedeutet, dass aus massenhaft erhobenen (Meta-)Daten mit Hilfe von Algorithmen gewissermaßen errechnet wird, welches Verhalten der Norm entspricht, und welches Verhalten als davon abweichend identifiziert wird, beispielsweise typische Bewegungsprofile von als Terrorist_innen identifizierten Personen. Ganz ähnlich funktionieren die primär aus der Wirtschaft bekannten Big-Data-Analysen.

Aus Mobilfunk-Metadaten werden also Bewegungs- und Kontaktprofile erstellt, um auf deren Basis Bewegungsmuster, typische Tagesroutinen, soziale Netze und das Reiseverhalten zu berechnen. Für diese Berechnungen sind demzufolge nicht nur gezielt erhobene Metadaten von Zielpersonen erforderlich. Genauso wichtig sind die Metadaten aller anderen Menschen, um eine möglichst große Datenbasis für die Bestimmung des normalen und des davon abweichenden Verhaltens zu haben.

1207) MAT A BND-49/1, Bl. 25 (VS-NfD)

1208) Vgl. https://www.youtube.com/watch?v=kV2HDM86XgI (Min. 18:00); The New York Review of Books vom 10. Mai 2014, „'We Kill People Based on Metadata'“; vgl. http://www.nybooks.com/daily/2014/05/10/we-kill-people-based-metadata/.

1209) *c't.* Magazin für Computertechnik vom 22. Januar 2016, „Data Mining für den Drohnenkrieg. Lexikon des NSA -Skandals: Skynet“, vgl. https://www.heise.de/ct/ausgabe/2016-3-Lexikon-des-NSA-Skandals-Skynet-3073842.html.

Für Programme wie Skynet gibt es gar keine unnützen Daten, denn alle erhobenen Daten – in diesem Fall aus einer festgelegten Region – verfeinern das gewünschte Ergebnis. Vor diesem Hintergrund muss die Behauptung der Bundesregierung, sie gebe Daten weiter, die aber nicht zur Tötung von Menschen genutzt werden dürfen, völlig neu geprüft werden, denn angesichts dieser neuen Form der Zielfindung werden alle übermittelten Daten mittelbar zur Tötung durch Drohnen genutzt.

Die von The Intercept veröffentlichten Folien zu Skynet basieren auf Daten aus Pakistan. Dort sollen Schätzungen zufolge zwischen 2004 und 2015 insgesamt 2500 bis 4000 Personen durch US-Drohnenangriffe getötet worden sein.

Der Zeuge *Berfuß*, zwischen 2011 und 2014 in der Abteilung Islamismus/Terrorismus des BfV zuständig u.a. für Auswertung und Beschaffung im Bereich Internet und danach Referatsgruppenleiter im Bereich Technische Aufklärung des BfV, gab im Ausschuss an, lediglich eine „sehr schwammige“ Vorstellung von Data-Mining zu haben, das Programm Skynet habe er gar nicht gekannt.[1210] Angesichts der technischen Entwicklungen und gerade auch solcher Veröffentlichungen wie denen zu Skynet wirft das mindestens Fragen auf, denen auch nach dem Abschluss des Untersuchungsausschusses nachzugehen sein wird.

5. Rechtliche Verantwortung der Bundesregierung für den US-Drohnenkrieg

Die bisherigen Erkenntnisse über das US-Drohnenprogramm und die die Auswahl der Ziele, insbesondere bei gezielten Tötungen, sowie im Hinblick auf die verursachten Opfer und zivilen Schäden führen zu dem Schluss, dass der von den Vereinigten Staaten geführte Drohnenkrieg mit dem Völkerrecht und menschenrechtlichen Anforderungen in überwiegendem Maße nicht vereinbar ist. Daraus leitet sich ein Verantwortungszusammenhang für die Bundesregierung her, soweit diese über die Bereitstellung des Militärstützpunktes Ramstein oder gar die Übermittlung von Daten für die Zielerfassung zum Drohnenkrieg der USA Beihilfe leistet. Diese nicht nur politische Verpflichtung der Bundesregierung folgt aus ihrer verfassungsrechtlichen Stellung als für die

1210) *Berfuß,* Protokoll-Nr. 96 I, S. 31 f.

Außenpolitik verantwortliches Exekutivorgan, aus grundrechtlichen Schutzpflichten sowie aufgrund völker- und menschenrechtlicher Anforderungen.

Die mit dem Drohnenkrieg einhergehende Ausweitung der Kampfzone und Infragestellung rechtlicher Standards bereiten den Boden für neue Dimensionen der Gewaltanwendung mit – immer häufiger automatisierten – militärischen Mitteln, die den völkerrechtlichen Verpflichtungen zur Mäßigung und Einhegung des Krieges zu wider laufen und deswegen auch mit dem Friedensgebot des Grundgesetzes unvereinbar sind.

Im folgenden Abschnitt wird zunächst der verfassungs- und völkerrechtliche Rechtsrahmen für die Verantwortung der Bundesregierung skizziert, anschließend der US-Drohnenkrieg am Maßstab des Völkerrechts bewertet und dargestellt, warum das Unterlassen der Bunderegierung im Hinblick auf die Ergreifung wirksamer Maßnahmen zur Aufklärung, Kontrolle und Unterbindung völkerrechtswidriger Drohnenangriffe zugleich einen Verstoß gegen ihre verfassungsrechtlichen Pflichten darstellt.

a) (Mit-)Verantwortung der Bundesregierung für den US-Drohnenkrieg

Der US-Drohnenkrieg begründet vor allem in Folge der essentiellen Bedeutung der US-Militärbasis Ramstein einen Verantwortungszusammenhang für die Bundesregierung, den diese nicht wahrhaben will. Er folgt sowohl aus verfassungs- wie völkerrechtlichen Verpflichtungen der Bundesregierung, friedensstörenden und völkerrechtswidrigen Gewaltanwendungen entgegen zu wirken und auf seinem Hoheitsgebiet bzw. für seine Exekutivorgane auszuschließen.

aa) Verfassungsrechtliche Verpflichtungen

Das Grundgesetz steht der Anwendung von Waffengewalt durch ausländische Streitkräfte oder Nachrichtendienste nicht gleichgültig gegenüber. Es konstituiert den Staat als eine umfassende Friedens- und Ordnungsmacht und begründet in diesem verfassungsrechtlichen Rahmen Verantwortungs- und Zurechnungssphären für die staatliche Gewalt. Im Hinblick auf den Einsatz bewaffneter Kampfdrohnen können diese sich sowohl aus dem Friedensgebot des Grundgesetzes als auch aus dem Staatsorganisationsrecht, vor allem aber aus den Grundrechten hergeleitet werden. Dabei steht

das Grundgesetz tatbestandlich eng mit den allgemeinen völkerrechtlichen Bestimmungen in Zusammenhang, begründet aber darüber hinaus weitergehende innerstaatliche Bindungen für die Bundesregierung als das Völkerrecht.

aaa) Das Friedensgebot des Grundgesetzes

Das Friedensgebot des Grundgesetzes wird als Staatszielbestimmung verstanden, dessen normativer Gehalt umstritten ist.[1211] Es ergibt sich aus einer Reihe programmatischer, struktureller und inhaltlicher Einzelbestimmungen:

– Der Präambel, die vom Willen der Bevölkerung berichtet, „dem Frieden der Welt zu dienen“,

– dem in Art. 1 Abs. 2 GG ausgesprochen Bekenntnis zu den „Menschenrechten als Grundlage jeder menschlichen Gemeinschaft, des Friedens und der Gerechtigkeit in der Welt“,

– dem Verbot des Führens oder Vorbereitens von Angriffskriegen und von „Handlungen, die geeignet sind und in der Absicht vorgenommen werden, das friedliche Zusammenleben der Völker zu stören“ in Art. 26 Abs. 1 GG,

– dem Verbot von Vereinigungen, die sich „gegen den Gedanken der Völkerverständigung richten“ in Art. 9 Abs. 2 GG,

– die in Art. 20 Abs. 3 GG normierte Bindung an „Recht und Gesetz“ und

– an die „allgemeinen Regeln des Völkerrechts“ (Art. 25 GG), insbesondere das Gewaltverbot als allgemeiner Grundsatz des Völkerrechts,

– dem in Art. 24 Abs. 2 GG für die Einordnung in ein System gegenseitiger kollektiver Sicherheit ausgesprochen Vorbehalt „zur Wahrung des Friedens“,

1211) Skeptisch *Alexander Proelß* (2013): Das Friedensgebot des Grundgesetzes, in: Isensee/Kirchhoff (Hg.), Handbuch des Staatsrechts, Band XI, 3. Auflage, C.F. Müller Heidelberg, S. 63-88 (65, 87); progressiv gewendet in der einfachgesetzlichen Ausgestaltung aber kritisch beleuchtet bei Dieter Deiseroth (2009): Das Friedensgebot des Grundgesetzes und der UN-Charta, Betrifft Justiz Nr. 99,S. 143-149.

– die in Art. 24 Abs. 3 GG angelegte, aber noch immer nicht vollständig erfolgte Unterwerfung unter die obligatorische Gerichtsbarkeit des Internationalen Gerichtshofs in Den Haag (IGH),

– der parlamentarischen Entscheidung über den Friedensschluss per Gesetz (Art. 115 l Abs. 3 GG) sowie

– dem in Art. 79 Abs. 1 Satz 2 GG ausgesprochenen Vorrang für solche völkerrechtlichen Verträge, „die eine Friedensregelung" oder „die Vorbereitung einer Friedensregelung […] zu dienen bestimmt sind".

Zentral ist hierbei das verfassungsrechtliche Prinzip des friedlichen Zusammenlebens der Völker in Art. 26 GG als Konkretisierung des Friedengebots.[1212] Es knüpft eng an die in Art. 24 angelegte internationale Zusammenarbeit und in Art. 25 verbürgte Völkerrechtsfreundlichkeit der Verfassung an und beinhaltet ein Verdikt gegen die militärische „Lösung" internationaler Streitfragen.[1213]

Lediglich zur Verteidigung dürfen militärische Instrumente eingesetzt werden, wie auch Art. 87a Abs. 1 Satz 1 GG verdeutlicht.[1214] Art. 26 GG erhebt damit das völkerrechtliche Gewaltverbot auf eine gleichrangige und gleichlaufende verfassungsrechtliche Ebene. Einfachgesetzlich sollen „Handlungen, die geeignet sind und in der Absicht vorgenommen werden, das friedliche Zusammenleben der Völker zu stören" unter Strafe gestellt werden. Tatsächlich aber setzt § 80 StGB dies in der Praxis nur unvollständig um.[1215]

Ein weiteres zentrales Element des Friedensgebotes des GG ist die normierte Bindung an „Recht und Gesetz" (Art. 20 Abs. 3 GG) und an die „allgemeinen Regeln des Völ-

1212) BVerfGE 47, 327 (382).

1213) *Jarass* (2002), in: *Jarass/Piroth*, GG, Kommentar, Art. 26 Rn. 1. Zum unterhalb der Verfassung, aber vorrangig vor den Bundesgesetzen geltenden Völkerrecht gehört u.a. der „Vertrag über die Ächtung des Krieges" (*Briand-Kellog-Pakt*) vom 27. August 1928, in dem die Vertragsparteien „den Krieg als Mittel für die Lösung internationaler Streitfälle verurteilen" und auf ihn „als Werkzeug nationaler Politik in ihren gegenseitigen Beziehungen verzichten".

1214) BVerwGE 83, 60 (65).

1215) Kritisch dazu *Deiseroth* (2009): Das Friedensgebot des Grundgesetzes und der UN-Charta, Betrifft Justiz Nr. 99,S. 143–149

kerrechts“ (Art. 25 GG), die unmittelbare Auswirkungen für alle Rechtsbereiche entfalten.[1216] Danach muss das gesamte deutsche Recht völkerrechtskonform ausgelegt und angewendet werden,[1217] dürfen deutsche Stellen weder im In- noch im Ausland oder in internationalen Gremien, etwa der EU oder der NATO, an Aktionen oder Beschlüssen mitwirken, die einen Verstoß gegen geltendes Völkerrecht beinhalten oder bewirken.[1218] Und sind daher Hoheitsakte – z. B. auch gegenüber Soldaten erteilte Befehle –, die gegen Art. 25 GG verstoßen, verfassungswidrig und müssen nicht befolgt werden.[1219]

bbb) Verantwortung der Bundesregierung für die Außenpolitik

Die Ausübung der dem Bund gemäß Art. 32 GG zukommenden Zuständigkeit für die auswärtige Gewalt „ist eine Funktion der Regierung“.[1220] In Anknüpfung an traditionelle staatsrechtliche Auffassung überantwortet das Bundesverfassungsgericht (BVerfG) der Regierung „im Bereich auswärtiger Politik einen weit bemessenen Spielraum zu eigenverantwortlicher Aufgabenwahrnehmung“.[1221] Dementsprechend ist „die Rolle des Parlaments schon aus Gründen der Funktionsgerechtigkeit in diesem Bereich beschränkt“.[1222]

Mit dem weiten Einschätzungs- und Gestaltungsspielraum der Bundesregierung für die Außenpolitik korrespondiert jedoch spiegelbildlich die Kontroll- und Informationsbefugnis des Parlaments und seiner Gremien.[1223] Demgemäß können auch völkerrechtliche Verpflichtungen keine unmittelbare Schranke der parlamentarischen Kompetenzen begründen, da sie als solche keinen Verfassungsrang besitzen.[1224] Aus dem

---

1216) *Deiseroth* (2009): Das Friedensgebot des Grundgesetzes und der UN-Charta, Betrifft Justiz Nr. 99,S. 143–149.

1217) Vgl. BVerGE 58, 1 (34); 59, 63 (89); 63, 343 (373); 64, 1 (20); 75, 1 (18f); 109, 13 (23); 111, 307.

1218) BVerwG, NJW 1988, 1462 f.

1219) Vgl. BVerwG, Urt. v. 21.6.2005 – BVerwG 2 WD 12.04 – Eu GRZ 2005, 636 (648) m.w.N.

1220) BVerfGE 1, 372 (394); vgl. auch BVerfGE 68, 1 (85 f.); 90, 286 (357).

1221) BVerfG, Beschluss des Zweiten Senats vom 13. Oktober 2016, Az. 2 BvE 2/15, Rn. 120.

1222) Vgl. BVerfGE 104, 151 (207); 131, 152 (195).

1223) *Christoph Möllers* (2017): Von der Kernbereichsgarantie zur exekutiven Notstandsprärogative: zum BND-Selektoren-Beschluss des BVerfG, JZ 6/2017, S. 271 ff.

1224) BVerfG, Beschluss des Zweiten Senats vom 13. Oktober 2016, Az. 2 BvE 2/15, https://www.bverfg.de/e/es20161013_2bve000215.html, Rn. 112.

Kontrollrecht des Bundestages folgt die Informationsverpflichtung der Bundesregierung, die unter bestimmten Voraussetzungen, insbesondere im Zusammenhang mit Untersuchungsausschüssen, auch die Herausgabe oder Ermittlung geheim gehaltener Informationen betreffen kann.

Allerdings schrieb das BVerfG in seiner neuesten, aus Anlass dieses Untersuchungsausschusses geprägten und oben bereits kritisierten Rechtsprechung der Bundesregierung ein schutzwürdiges Interesse „an funktionsgerechter und organadäquater Aufgabenwahrnehmung“ zu,[1225] das ausgerechnet im Bereich der parlamentarischen Kontrolle geheimdienstlicher Maßnahmen Ausnahmen vom Informationsanspruch rechtfertigen können soll.[1226] Die Befugnis, unter Bezugnahme auf diese Rechtsprechung Informationen zurück zu halten, ist allerdings aufwändig begründungspflichtig und betrifft zudem abgeschlossener Sachverhalte. Soweit eine akute Verletzung verfassungs- und völkerrechtlicher Bestimmung im Raum steht, die mit einem Unterlassen oder Unterstützen von Regierungsstellen einhergeht, ist die Aufklärungs- und Kontrollfunktion des Parlaments aktiviert.

ccc) Grundrechtliche Schutzansprüche

Nach Art. 1 Abs. 3 GG ist die Ausübung jeglicher hoheitlichen Gewalt an die Grundrechte gebunden. Eine territoriale Beschränkung ist nicht vorgesehen. Auf diese wird die deutsche Staatsgewalt durch das Grundgesetz verpflichtet, unabhängig davon, wo sich ihre Handlungen oder Unterlassungen konkret auswirken. Entsprechend verpflichten die Grundrechte die deutsche Staatsgewalt auch bezüglich im Ausland gelegener Schutzgüter, soweit ein hinreichend konkreter Bezug zur eigenen hoheitlichen Tätigkeit vorliegt.

1225) BVerfG, Beschluss des Zweiten Senats vom 13. Oktober 2016, Az. 2 BvE 2/15, https://www.bverfg.de/e/es20161013_2bve000215.html, Leitsatz 4.

1226) Zur Kritik: *Christoph Möllers* (2017): Von der Kernbereichsgarantie zur exekutiven Notstandsprärogative: zum BND-Selektoren-Beschluss des BVerfG, JZ 6/2017, S. 271 ff.; *Jelena von Achenbach/ Wolfgang Nešković* (2016): Selektoren-Urteil des BVerfG: Karlsruhe verzwergt das Parlament, verfassungsblog.de vom 21. November 2016; *Heiner Busch* (2017): Informationsrechte des Parlaments ausgehöhlt, in: *T. Müller-Heidelberg* u. a. (Hrsg.): Grundrechte-Report 2017, S. 175 ff.

Ein solcher Bezug ist auch in der Rechtsprechung[1227] für die Rolle Ramsteins im US-Drohnenkrieg angenommen worden. Damit können sich auch nicht-deutsche Personen auf die Grundrechte des Grundgesetzes berufen, die als Menschenrechte verbürgt sind und in Folge der Ermöglichung von Drohneneinsätzen über die Relaisstation Ramstein tangiert werden. Der Schutzbereich des Artikel 2 Absatz 1 GG ist – mindestens im Wege der völkerrechtsfreundlichen Auslegung der Grundrechte, die einen menschenrechtlichen Charakter haben – durch die extraterritoriale Wirkung der Grundrechte auch für die im Ausland befindliche Ausländer_innen eröffnet, soweit sie von deutschen Hoheitsakten oder deren pflichtwidriger Unterlassung betroffen sind.

In erster Linie gilt das für das in Art. 2 Abs. 2 Satz 1 GG versprochene Recht auf Leben und körperliche Unversehrtheit. Daraus folgt zunächst ein Abwehranspruch gegen den Staat, Handlungen zu unterlassen, die darauf ausgehen oder im Ergebnis bewirken, dass das Leben eines Menschen konkret gefährdet werden kann – z.B. die Übermittlung von Telefonnummer, die der Ortung durch Drohnen dienen können. Es kann allerdings auch Schutzansprüche vermitteln, die den Staat aus der Passivität des Unterlassens herausholt und zu einem aktiven Tätigwerden verpflichtet. Die Reichweite solcher grundrechtlichen Schutzpflichten insbesondere hinsichtlich konkreter Handlungspflichten der Exekutive ist zwar umstritten, klar ist aber, dass ein Untätigbleiben gegen das grundrechtliche Untermaßverbot verstößt.

Im Hinblick auf den Einsatz von Drohnen kommt darüber hinaus eine Verletzung der Menschenwürde in Betracht, wenn die Betroffenen von Drohnenangriffen dadurch ihrer Subjektstellung beraubt und ohne eigene Einflussmöglichkeit zum „bloßen Objekt“ hoheitlicher Zwecksetzung und Maßnahmenzurechnung werden[1228]. So führte das *BVerfG* im Zusammenhang mit dem für mit der Menschenwürde für unvereinbar erklärten Gesetz zum Abschuss von Passiermaschinen im Falle einer terroristischen Entführung aus:

> „Dem Staat ist es im Hinblick auf dieses Verhältnis von Lebensrecht und Menschenwürde einerseits untersagt, durch eigene Maßnahmen

1227) VG Köln, Urteil vom 27. Mai 2015 – 3 K 5625/14 –, juris Rn. 35, in Zeitschrift für Datenschutz 2016, 402-404.

1228) BVerfGE 27, 1 (6); 45, 187 (228); 96, 375 (399), https://www.bverfg.de/e/rs19971112_1bvr047992.html.

> unter Verstoß gegen das Verbot der Missachtung der menschlichen Würde in das Grundrecht auf Leben einzugreifen. Andererseits ist er auch gehalten, jedes menschliche Leben zu schützen. Diese Schutzpflicht gebietet es dem Staat und seinen Organen, sich schützend und fördernd vor das Leben jedes Einzelnen zu stellen; das heißt vor allem, es auch vor rechtswidrigen An- und Eingriffen von Seiten Dritter zu bewahren. Ihren Grund hat auch diese Schutzpflicht in Art. 1 Abs. 1 Satz 2 GG, der den Staat ausdrücklich zur Achtung und zum Schutz der Menschenwürde verpflichtet.“[1229]

Was konkret Inhalt der staatlichen Schutzpflicht ist, ergibt sich aus dem grundrechtlichen Gefährdungszusammenhang. Allerdings ist hier zu berücksichtigen, dass der Einsatz von Waffengewalt in der Regel zum absoluten Substanzverlust, nämlich dem Verlust des Lebens führt, weswegen effektive Maßnahmen zur Abwendung dieser Gefahr ergriffen werden müssen. Einfach gesetzlich wird diese Verpflichtung zum Beispiel in dem Verbot der Übermittlung personenbeziehbarer Daten an ausländische Stellen ausgedrückt, wenn die Betroffenen dadurch der Gefahr von politischer Verfolgung, Folter und Tod ausgesetzt werden (vgl. § 19 Abs. 3 Satz 2 BVerfSchG, auf den auch § 24 Abs. 2 BNDG verweist).[1230]

Da bei den von den USA geflogenen Drohneneinsätzen insbesondere im Zusammenhang mit gezielten Tötungen nicht ohne weiteres davon ausgegangen werden kann, dass diese nur in Kriegsgebieten gegen völkerrechtlich als Kombattanten eingestufte Personen eingesetzt werden, sondern im Rahmen der Terrorbekämpfung durch die Geheimdienste zur extra-legalen Hinrichtung verwendet werden, ist hiervon das aus dem Rechtsstaatsprinzip folgende Recht auf effektiven Rechtsschutz und einen fairen Prozess (Art. 19 Abs. 4 GG) und das Verbot der Todesstrafe (Art. 102 GG) betroffen

---

1229) BVerfGE 115, 118 (152) m.w.N., https://www.bverfg.de/e/rs20060215_1bvr035705.html

1230) Vgl. *Bernadette Droste* (2007), Handbuch des Verfassungsschutzrechts, S. 529; *Christoph Gusy* (2014), in: Schenke/Graulich/Ruthig, Sicherheitsrecht des Bundes, § 9 BNDG Rn. 7; *Eric Töpfer* (2013): Informationsaustausch zwischen Polizei und Nachrichtendiensten strikt begrenzen. Konsequenzen aus dem Urteil des Bundesverfassungsgerichts zur Antiterrordatei, Policy Paper des Deutschen Instituts für Menschenrechte, S. 18; *Michael Plöse* (2014): Was Karlsruhe nicht verbietet, macht Berlin nur dreister, Anmerkungen zur Änderung des Antiterrordateigesetzes, Vorgänge Nr. 206/207, S. 122–134 (128).

und gebietet grundsätzlich staatliche Verfahrens- und Schutzgewährung, soweit sie Gewahrsam begründet. Ihrer Verantwortung für die Durchführung rechtsstaatlicher Verfahren kann sie sich nicht durch die Zulassung präventiver Tötungen entziehen.

Es sei darauf hingewiesen, dass auch im US-amerikanischen Kontext die Frage der Verfassungsmäßigkeit der US-Drohnenangriffe umstritten diskutiert wird.[1231]

bb) Völkerrechtliche Verpflichtungen

Im Rahmen der gezielten Tötungen durch Drohnenangriffe folgt eine Verantwortung der Bundesregierung zudem aus völkerrechtlichen Vorgaben, namentlich dem Gewaltverbot der UN-Charta, den Anforderungen des humanitären Völkerrechts sowie den Gewährleistungen der internationalen Menschenrechtspakte.

Im Rahmen des Gewaltverbots nach Art. 2 Abs. 4 der UN-Charta stellt sich die Frage, ob der Einsatz von Drohnen als militärische Maßnahme in einem weltweiten „Krieges gegen den Terror“ und die Beteiligung hieran eine Verletzung des Völkerrechts darstellt oder gerechtfertigt ist (*ius ad bellum*).

Die Frage nach der Anwendbarkeit des Humanitären Völkerrechts (*ius in bello*) und der sich aus ihm ergebenden Beschränkung für den Einsatz militärischer Waffengewalt wirft die Frage auf, ob es sich bei den Krisengebieten, in denen Waffengewalt durch den Einsatz von Drohnen ausgeübt wird, völkerrechtlich um sog. bewaffnete Konflikte handelt, in denen feindliche Kombattanten in dem vom Humanitären Völkerrecht gesetzten Rahmen mit Waffengewalt bekämpft werden können. Außerhalb von bewaffneten Konflikten ist der Einsatz von Drohnen zur gezielten Tötung von Menschen ebenso wie die Ausübung spezifisch militärischer Waffengewalt nämlich nur in eng begrenzten Ausnahmefällen unmittelbarer Gefahr für Leib und Leben anderer Menschen zulässig, ansonsten haben polizei- und strafrechtliche Maßnahmen gegenüber militärischen Optionen Vorrang.

Im Rahmen dieser Prüfung stellt das Gewährenlassen oder gar die Unterstützung des US-Drohnenkrieges durch die Bundesregierung zugleich als ein Verstoß gegen das

1231) Vgl. *Powell, J.* (2016): Targeted Americans. The Constitutionality of the U.S. Drone War (Oxford University Press, Oxford).

grundgesetzliche Friedensgebot dar, wenn sich der Drohneneinsatz auch nur in einer signifikanten Anzahl von Fällen als völkerrechtswidrig erweist. Schließlich verpflichten die internationalen Menschenrechtspakte, insbesondere der Internationale Pakt über bürgerliche und politische Rechte (IPbpR) und die Europäische Menschrechtskonvention, sowie das Völkerstrafrecht (vgl. Völkerstrafgesetzbuch) zur Gewährleistung von Mindestanforderungen zum Schutz des Lebens unabhängig davon, ob es sich um einen bewaffneten Konflikt handelt oder nicht.

b) Bewertung des US-Drohneneinsatzes

Zusammenfassend lässt sich feststellen: In zunehmender Maße stellen sich die Einsätze mit Kampfdrohnen durch die USA in Folge der Auflösung staatlicher Gewalt und der sich anhaltend ändernden Kräfteverhältnisse, Konfliktlinien und -parteien in den Einsatzgebieten als völkerrechts- und menschenrechtswidrige Kampfhandlungen außerhalb von bewaffneten Konflikten dar. In diesem Rahmen ist der Einsatz von militärischer Waffengewalt an strenge Maßstäbe gekoppelt und nur im Einzelfall zulässig. Das gilt in besonderem Maße für den Einsatz von Kampfdrohnen, die als neue Waffentechnologie und Kampfmethode auch im Rahmen von bewaffneten Konflikten völkerrechtlich an strengere Einsatzvoraussetzungen gebunden sind, um zivile Opfer zu schonen und Kriegshandlungen in einem rechtlichen Rahmen zu halten. Die bisherige Einsatzpraxis der USA lassen eine solche Einzelfallprüfung überwiegend vermissen.

Angesichts der entscheidenden Bedeutung, den der US-Militärstützpunkt Ramstein als Relaisstation für den US-Drohnenkrieg einnimmt, trifft die Bundesregierung eine strikte Mitverantwortung, die sie von Verfassungs wegen zur Ergreifung effektiver Maßnahmen der Aufklärung, parlamentarischen Information sowie Einwirkung gegenüber den militärischen Bündnispartnern in den USA verpflichtet. Weitergehend muss sie ihre eigene Übermittlungspraxis im Hinblick auf den Austausch von geheimdienstlichen Informationen überprüfen, um sicher zu stellen, dass übermittelte Daten nicht zur Grundlage illegaler Drohneneinsätzen werden.

Im Einzelnen: Hinsichtlich der Frage nach der Rechtmäßigkeit einer im Rahmen eines Drohnenangriffs ausgeführten gezielten Tötung kommen wie dargestellt drei völkerrechtliche Bereiche in Betracht: das Friedensvölkerrecht, das humanitäre Völkerrecht

und die Menschenrechte. Abgesehen von den Menschenrechten ist nicht jeder Einzelfall nach den Prüfungsmaßstäben der übrigen Rechtsbereiche zu beurteilen. Allerdings kommen in einigen Fallkonstellationen alle Rechtsregime nebeneinander zur Anwendung – etwa bei gezielten Tötungen mittels Drohnenangriffen durch einen Staat auf dem Hoheitsgebiet eines anderen Staates ohne dessen Einwilligung, im Rahmen von bewaffneten Konflikten oder bei punktueller Gewaltanwendung.[1232] Liegt hingegen die Einwilligung des Staates vor, auf dessen Gebiet Drohnenangriffe stattfinden, so sind allein humanitär-völkerrechtliche und menschenrechtliche Prüfungsmaßstäbe heranzuziehen.

Im Hinblick auf den sog. US-Drohnenkrieg ist dabei wie folgt zu differenzieren:

> „Tödliche Drohnenangriffe werden momentan auf zweierlei Weise realisiert: Durch Geheimdienste oder durch Streitkräfte. Der Hauptgrund hierfür liegt darin, dass Streitkräfte nur in bewaffneten Konflikten tätig werden, Geheimdienste aber vor allem im Bereich der Gefahrenabwehr, etwa im Rahmen der Bekämpfung des internationalen Terrorismus. Die Unterscheidung zwischen dem Vorliegen eines bewaffneten Konflikts und Gefahrenabwehr- oder Strafverfolgungsmaßnahmen ist allerdings von zentraler Bedeutung, da im bewaffneten Konflikt das Rechtsregime des humanitären Völkerrechts anwendbar ist, der anderes Recht teilweise verdrängt. Insbesondere gelten für gezielte Tötungen als Kriegshandlungen im humanitären Völkerrecht niedrigere Schranken als für die Anwendung tödlicher Gewalt durch Polizei und andere zivile Sicherheitskräfte.“1233

Vor dem Hintergrund dieser rechtlich schwierigen Bewertungslage ist der Bundesregierung vorzuwerfen, dass sie mit ihren hierzu vertretenen Rechtsauffassungen hinter

---

1232) So *Kapaun, N.* (2014): Völkerrechtliche Bewertung gezielter Tötungen nicht-staatlicher Akteure (Kölner Schriften zum Friedenssicherungsrecht), (Book on Demand), S. 323.

1233) *Andreas Schüller* (2013): Rechtsschutzmöglichkeiten bei gezielten Tötungen durch Drohnen, S. 2 f., Download: http://www.ialana.de/files/pdf/nato-kongress-doku/_Rechtsschutzmglichkeiten_bei_gezielten_Ttungen_durch_Drohnen_Andreas_Schueller.pdf (abgerufen am 16. Juni 2017).

den gegenwärtigen völkerrechtlichen Diskussionen über die Rechtmäßigkeit von Drohneneinsätzen zurückbleibt. Insbesondere betrifft dies die folgenden Anforderungen:

- Anwendung des Friedensvölkerrecht (*ius ad bellum*) und des humanitären Völkerrechts (*ius in bello*),
- Menschenrechtliche Verpflichtungen bei Kampfhandlungen,
- Vereinbarkeit des Einsatzes bewaffneter Drohnen mit dem Völkerrecht,
- Zulässigkeit gezielter Tötungen in- und außerhalb von bewaffneten Konflikten,
- Qualifizierung bewaffneter Gruppen als legitime militärische Ziele,
- Reichweite der Verpflichtung zur Minimierung von zivilen Opfern und Kollateral-Schäden (Unterscheidungsgebot und Verbot unnötigen Leidens).

aa) Recht zum Krieg (ius ad bellum)

Als erstes ist auf das in Art. 2 Abs. 4 der UN-Charta verbürgte Gewaltverbot hinzuweisen, das zwingendes Völkerrecht ist (*ius cogens*). Gemäß dieser Vorschrift ist jede Androhung und Anwendung von Gewalt in den internationalen Beziehungen der Staaten untereinander verboten.

Gegenstand des Gewaltverbots sind die territoriale Unversehrtheit, die politische Unabhängigkeit eines Staates und die Ziele der Vereinten Nationen. Das Gewaltverbot entfällt dann, wenn vom angegriffenen Staat eine wirksame Einladung zur Intervention vorliegt, deren grundsätzliche Zulässigkeit jedoch umstritten ist und wenn überhaupt nur unter strengsten Voraussetzungen diskutiert wird.[1234]

1234) *Städele, J.P.* (2014): Völkerrechtlicher Implikationen des Einsatzes bewaffneter Drohnen (Duncker & Humblot, Berlin), S. 158. In diesem Sinne ist auch der Ansicht des Referats V I 2 des BMI zu widersprechen, wonach neben der Zustimmung eines Staates noch eine weitere Ausnahme vom Gewaltverbot gegeben sei, wenn der Staat „das Agieren nichtstaatlicher Akteure von seinem Staatsgebiet aus nicht unterbinden könne oder wolle“.

Diese Problematik tritt im Falle der von der *CIA* zwischen 2007 und 2012 durchgeführten Drohnenangriffe im pakistanischen Nord-Wasiristan besonders hervor, denn diesen wurde laut US-Argumentation ein Einverständnis der pakistanischen Behörden zugrunde gelegt.[1235]

Das Gewaltverbot bindet in erster Linie Staaten und erfasst daher grundsätzlich nicht die Gewalt von oder gegen nicht-staatliche Akteure als solche, zum Beispiel organisierte bewaffnete Gruppen. Diese müssen vielmehr einem Völkerrechtssubjekt zugerechnet werden können. Im Fall der Terroranschläge auf das World Trade Center in den USA 2001 wurde allerdings die von der Al-Qaida ausgeübte nicht-staatliche Gewalt der afghanischen Taliban-Regierung zugerechnet, weil diese der Terrororganisation Schutz gewährt hatte (sog. „safe-haven-Doktrin"). Entsprechend wurde auch ein Selbstverteidigungsrecht der USA diskutiert.

Eine Durchbrechung des Gewaltverbots ist nämlich in zwei Fällen gerechtfertigt: Entweder handelt es sich um eine UN-Maßnahme nach Art. 39 ff. UN-Charta oder um die Ausübung des Selbstverteidigungsrechts nach Art. 51 UN-Charta, das auch kollektiv ausgeübt werden kann. Vor allem letzteres stellt einen wichtigen Ausnahmetatbestand dar. Nach dieser Vorschrift (Art. 51 UN-Charta) wird das Recht eines UN-Mitgliedstaates zur individuellen oder kollektiven Selbstverteidigung im Falle eines bewaffneten Angriffs durch die Charta nicht beeinträchtigt, zumindest

> „bis der Sicherheitsrat die zur Wahrung des Weltfriedens und der internationalen Sicherheit erforderlichen Maßnahmen getroffen hat."

Voraussetzung für die Ausübung des Selbstverteidigungsrechts ist ein gegenwärtiger und anhaltender „bewaffneter Angriff" auf einen Mitgliedsstaat der UN, was der Staat zu beweisen hat, der sich auf das Selbstverteidigungsrecht beruft.[1236] In diesem Zusammenhang ist insbesondere der sogenannte globale Krieg gegen den Terrorismus

---

1235) Siehe auch das Urteil des Peshawar High Court v. 11.4.2013, Nr. 1551-P/2012, in dem das Oberste Gericht die von CIA auf pakistanischem Boden durchgeführten Drohnenangriffen als Kriegsverbrechen feststellte und die Regierung aufforderte, ihre staatliche Souveränität gegenüber den USA durchzusetzen.

1236) *Städele, J.P.* (2014): Völkerrechtlicher Implikationen des Einsatzes bewaffneter Drohnen (Duncker & Humblot, Berlin), S. 89.

(„global war on terror“), wie ihn die USA als Ausübung ihres Selbstverteidigungsrechts zu führen beansprucht, höchst umstritten diskutiert.[1237]

War der Vergeltungsangriff auf das Taliban-Regime in Afghanistan 2001 im Beschluss des Sicherheitsrates über die Resolution 1368 als ein Akt der Selbstverteidigung wenigstens angelegt und die Mission der *ISAF*-Schutztruppe jedenfalls durch die Resolution 1386 völkerrechtlich abgesegnet, ist die Ausweitung der Kampfzone auf andere Staatsgebiete und auch innerhalb Afghanistans auf befriedete Bereiche alles andere als ohne Weiteres durch das Recht zur Selbstverteidigung gedeckt. Insoweit fehlt es schon an einem unmittelbaren, gegenwärtigen und anhaltenden Angriff auf das Staatsgebiet der USA bzw. eines *NATO*-Bündnispartners.[1238]

Auch der Mehrheitsbericht weist auf diese Rechtsauslegung der USA hin und hält fest, dass aus Perspektive der USA der Drohnenkrieg legitim sei. Damit hat es sein Bewenden. Eine Erörterung der grundsätzlichen Fragen nach der Rechtmäßigkeit der Kriegsführung mittels Drohnen und insbesondere von gezielten Tötungen fehlt. Dabei ist für die Frage nach der Verantwortung der *Bundesregierung* durchaus von Relevanz, ob die im Mehrheitsbericht dargestellte Sichtweise der US-Regierung völkerrechtlich Bestand haben kann. Denn eine Aufweichung dieser für die internationale Friedenswahrung zentralen völkerrechtlichen Frage öffnet Tür und Tor für eine Erosion des Kriegsvölkerrechts insgesamt. So berief sich Frankreich nach den Terroranschlägen in Paris 2015 auf sein Selbstverteidigungsrecht und rechtfertigte damit das Bombardement auf Stellungen des IS in Syrien und dem Irak, ohne dass hierzu von den jeweiligen Regierungen Einladungen ausgesprochen wurden oder ihnen diese nicht-staatlichen Akteure als eigene Einheiten zugerechnet werden könnten.[1239] In Großbritannien wird diskutiert, ob eine Selbstverteidigung des Vereinigten Königreichs nicht auch gegen Einzelpersonen, z.B. britische sogenannte Gefährder in Syrien ausgeübt werden dürfe,

---

1237) Vgl. *Jahn-Koch, I./Koch, M.*, Bewaffnete Drohnen – Teufelszeug oder Waffen wie andere?, in Delbrück, J. u.a. (Hg.) (2014): (Duncker & Humblot, Berlin), S. 284.

1238) Zu verneinen ist in diesem Zusammenhang die Frage, ob einzelne geringfügige Gewaltanwendungen kumuliert werden dürfen und somit doch als bewaffneter Angriff bewertet werden dürfen; dazu *Jahn-Koch, I./Koch, M.*, Bewaffnete Drohnen – Teufelszeug oder Waffen wie andere?, in Delbrück, J. u.a. (Hg.) (2014): (Duncker & Humblot, Berlin)., S. 97-100.

1239) Vgl. dazu *Alexander Schwarz* (2015): Die Terroranschläge in Frankreich – Ein Fall für das Recht auf Selbstverteidigung?, JuWissBlog vom 17. November 2015: https://www.juwiss.de/83-2015/ (abgerufen 8. Juni 2017).

ohne dass es sich überhaupt noch um eine nicht-staatliche bewaffnete Gruppe handeln muss.

bb) Humanitäres Völkerrecht (ius in bello)

aaa) Allgemein

Wenn man der Bundesregierung in ihrer Auffassung folgen würde und unterstellte, dass es sich bei den Einsatzgebieten der US-Drohnenangriffe um Konfliktzonen handelt, die im völkerrechtlichen Sinne als bewaffnete Konflikte gelten können, wären jedenfalls die Anforderungen des humanitären Völkerrechts (*ius in bello*) zu beachten. Dessen Ziel ist es,

> „die zerstöririschen Auswirkungen militärischer Gewalt auf die unmittelbar betroffenen Personen zu mildern, menschliches Leid im Krieg soweit möglich zu vermeiden und übermäßige Schäden an zivilen Gütern, insbesondere auch an der zivilen Infrastruktur, zu verhindern. Damit sucht es, die Sicherheit der vom Konflikt betroffenen Menschen zu stärken und ihre grundlegenden Rechte und Menschenwürde zu schützen.“[1240]

Die zentrale Frage lautet dabei, ob die Drohnenangriffe diese Anforderungen, insbesondere auch den Schutz der Menschenwürde, erfüllen.

Es ist jedoch darauf hinzuweisen, dass in der Regel nicht ohne weiteres davon ausgegangen werden kann, dass in den Einsatzgebieten bewaffneter US-Drohnen tatsächlich bewaffnete Konflikten bestehen. Vielmehr stellt sich der gezielte Einsatz von Waffengewalt gegen Terrorverdächtige als Gefahrenabwehrmaßnahme in Gebieten bestehender wenn auch begrenzter Staatlichkeit dar, der nach polizei- bzw. strafrechtlichen und damit strengeren Maßstäben zu messen wäre.

1240) *Daniel Thürer*, in *Hans-Peter Gasser/ Nils Melzer* (Hg.) (2012): Humanitäres Völkerrecht. Eine Einführung, 2. Überarb. Aufl., Nomos/Schulthess, Zürich, S. 22.

Die Anwendung des humanitären Völkerrechts setzt einen bewaffneten Konflikt voraus. Dazu müssen gegenseitig Kampfhandlungen geführt werden.[1241] Für die Arbeit des Ausschusses standen dabei vor allem nicht-internationale bewaffnete Konflikte im Mittelpunkt, z. B. in Pakistan.

Ein bewaffneter Konflikt gilt als nicht-international, wenn bewaffnete Auseinandersetzungen zwischen der Regierung eines Staates und aufständischen Gruppen, oder zwischen nicht-staatlichen Organisationen untereinander stattfinden (vgl. Artikel 8 Absatz 2 lit. f IStGH-Statut). Die rechtliche Grundlage für nicht-internationale bewaffnete Konflikte bilden hauptsächlich der gemeinsame Artikel 3 der vier Genfer Abkommen von 1949 und das Protokoll II. Ergänzt werden diese durch gewohnheitsrechtliche Vorschriften und durch allgemeine Grundsätze des humanitären Völkerrechts. Zutreffend verweist der Mehrheitsbericht auf die im gemeinsamen Artikel 3 der Genfer Abkommen enthaltene zwei Tatbestandsmerkmale eines nicht-internationalen bewaffneten Konfliktes. Erstens müssen die langanhaltenden (*protracted*) Kampfhandlungen eine gewisse Gewaltintensität erreicht haben; vereinzelte (gewalttätige) Aktionen reichen somit nicht aus. Zweitens verlangt ein nicht-internationaler bewaffneter Konflikt einen bestimmten Organisationsgrad der Konfliktparteien, der für staatliche Streitkräfte vorausgesetzt wird, nicht jedoch für nichtstaatliche bewaffnete Gruppen (siehe dazu unten (a)).

Hingegen gelten nach Artikel 1 Absatz 2 des Zusatzprotokolls II „Fälle innerer Unruhen und Spannungen wie Tumulte, vereinzelt auftretende Gewalttaten und andere ähnliche Handlungen“ nicht als nicht-internationale bewaffnete Konflikte. Rechtliche Maßstäbe für letztere sind daher in polizeirechtlichen Vorschriften zu suchen, die ihrerseits menschenrechtskonform angewendet werden müssen. Unter territorialen Gesichtspunkten kann von einem nicht-internationalen bewaffneten Konflikt die Rede sein, wenn die Auseinandersetzungen nicht nur innerhalb eines Staatsterritoriums stattfinden, sondern auf das Territorium eines Nachbarstaates ausgeufert sind.

Aus diesen Erläuterungen wird deutlich, dass die Feststellung der Bundesregierung, dass der „Konflikt in Afghanistan“ ein nicht-internationaler Konflikt sei, schlichtweg zu

---

1241) Vgl. Internationaler Gerichtshof für das ehemalige Jugoslawien, *Limaj*, Urt. v. 30.11.2005, Nr. IT-3-66-T, Rn. 169.

pauschal und nach völkerrechtlichen Maßstäben nicht haltbar ist. Denn der Bundesregierung obliegt es unter strengen Voraussetzungen, sorgfältig zu prüfen, ob zu einer bestimmten Zeit und in einem bestimmten Ort ein nicht-internationaler Konflikt vorliegt oder nicht. Eine Einzelfallprüfung eines Konflikts ist nach humanitär völkerrechtlichen Maßstäben mithin absolut notwendig.

Konkret bedeutet dies, dass einzelne grenzüberschreitende terroristische Gewaltakte an sich nicht schon als (transnationale) nicht-internationale Konflikte gelten können, wie menschenverachtend sie auch sein mögen. Nur eine konkrete und gegenwärtige Einzelfallprüfung kann den schnellen Änderungsdynamiken und den aktuellen Kräfteverhältnissen in den gegenwärtigen Konflikten Rechnung tragen. Dies ist besonders für den Jemen festzustellen, wo unterschiedliche Kräfte mit oder ohne Regierungsbeteiligung je nach Zeitpunkt einen unterschiedlichen Organisationsgrad aufweisen und dominierend oder gewalttätig waren. Die Bundesregierung genügt sich jedoch mit der pauschalen Feststellung, dass im Jemen ein bewaffneter Konflikt stattfände.

bbb) Anforderungen an den Einsatz bewaffneter Drohnen in bewaffneten Konflikten

(1) Drohnen als verbotene Mittel der Kriegsführung? – Die Position der Bundesregierung und die Kritik in der völkerrechtlichen Literatur

Ob es sich beim Einsatz bewaffneter Drohnen an sich bereits um ein Mittel verbotener Kriegsführung handelt oder deren Verwendung nur im konkreten Einzelfall gegen Bestimmungen des humanitären Völkerrechts oder internationale Pakte zum Schutze der Menschenrechte verstoßen kann, darüber wird in Politik, Literatur und vor Gerichten gestritten.

Der Leiter der Rechtsabteilung im Auswärtigen Amt, Ministerialdirektor *Michael Koch*, hob bei seiner Anhörung vor dem Ausschuss hervor, dass Drohnen als Waffentypus im Prinzip nicht völkerrechtswidrig seien. Anders als Chemiewaffen, Streubomben oder Laser unterlägen sie keiner Ächtung durch die Staatengemeinschaft. Die Drohne

sei keine Waffe, die „bei bestimmungsmäßigem Gebrauch regelmäßig zu völkerrechtswidrigen Ergebnissen“ führe.[1242] Die Rechtmäßigkeit von Drohnenattacken sei daher immer nur im Einzelfall zu beurteilen.

Demgegenüber wird häufig die Kritik geäußert, dass die Drohne eine enthemmende Wirkung entfalte, die das Geschäft des Tötens zu einem Videospiel macht.[1243] Hinzu komme die verwerfliche Art der asymmetrischen Kriegsführung, bei der Piloten von Drohnen keiner Lebensgefahr ausgesetzt sind.

Völkerrechtlich ist es nach Art. 36 des Protokoll I geboten, „neue Waffen oder neue Mittel oder Methoden der Kriegsführung“ auf ihre Völkerrechtskonformität hin zu prüfen. Damit verbindet sich ein Verbot des Einsatzes solcher Technologien, wenn festgestellt wird, dass deren „Verwendung stets oder unter bestimmten Umständen“ durch eine „Regel des Völkerrechts verboten wäre“. Wenngleich die Drohne nicht als solche an sich eine Waffe darstellt und die von den Drohnen aus abgefeuerten Raketen oder Präzisionsbomben völkerrechtlich zulässig sind, stellt gerade die Verbindung beider Bestandteile eine neue Dimension der Kriegsführung dar. Hauptkritikpunkt ist weiterhin, dass Drohnenangriffe erhebliche Verluste unter der unbeteiligten Zivilbevölkerung verursachen, die im Hinblick auf das Verbot überflüssigen Leidens und unnötiger Verletzungen sowie unter dem Gesichtspunkt des Unterscheidungsgebots eine Verletzung des humanitären Völkerrechts darstellen können.[1244] Der letztgenannte Grundsatz verlangt zum Schutze der Zivilbevölkerung eine Differenzierung zwischen zulässigen militärischen Zielen und unzulässigen zivilen Personen und Objekten. Der erstgenannte stellt jeden Einsatz unter den Vorbehalt einer Verhältnismäßigkeitsabwägung, die ausschließen soll, dass Verluste unter der Zivilbevölkerung oder die Beschä-

---

1242) Dazu *Michael Koch*, Protokoll-Nr. 80 I, S. 31

1243) Dazu *Jahn-Koch, I./Koch, M.*, Bewaffnete Drohnen – Teufelszeug oder Waffen wie andere?, in Delbrück, J. u. a. (Hg.) (2014): (Duncker & Humblot, Berlin), S. 268 ff. m.w.N.

1244) International Court of Justice, Legality of the Threat or Use of Nuclear Weapons, Gutachten vom 8.7.1996, ICJ Reports, 1996, S. 226 ff.; vgl. Robert Frau, Der Einsatz von Drohnen, Eine völkerrechtliche Betrachtung, Vereinte Nationen 3/2013, S. 99 (102).

digung ziviler Objekte gegenüber dem erwarteten konkreten und unmittelbaren militärischen Vorteil in deutlichem Missverhältnis steht.[1245] Dabei werden die Frage aufgeworfen, ob der Drohnenangriff zwangsläufig zivile Personen in der Nähe von vermeintlichen oder bekannten Kämpfern treffen wird und ob die Zielauswahl von zivilen Personen als solche völkerrechtlich zu beanstanden ist.[1246]

Außerdem ist dem Einsatz von Kampfdrohnen vorzuwerfen, dass er überwiegend als Instrument der höchst umstrittenen „gezielten Tötung“[1247] *(targeted killing)* dient. Damit erweist sich die Drohne nicht selten als ein Hinrichtungsinstrument, das verborgen und auf unsicherer und unbekannter Grundlage Personen ohne Gerichtsverfahren liquidiert.[1248] In diesem Sinne stellen gezielte Tötungen außerhalb eines bewaffneten Konflikts, etwa in Pakistan und maßgeblich auch in Jemen, eklatante Verletzungen des Rechts auf Lebens nach Art. 6 des Internationalen Pakts über bürgerliche und politische Rechte (IPbpR) dar.

Im Rahmen eines nicht-internationalen bewaffneten Konflikts ist eine gezielte Tötung nur unter sehr strengen kumulativen Voraussetzungen nicht zu beanstanden: Die zu liquidierende Person muss zunächst ein legitimes Ziel sein, also Mitglied einer „organisierten bewaffneten Gruppe“[1249] oder als Zivilist „unmittelbar an Feindseligkeiten“ beteiligt sein.[1250] Die Tötung darf nicht „unterschiedslos“ geführt werden und unterliegt zudem dem Exzessverbot.[1251] Des Weiteren muss die gezielte Tötung „militärisch notwendig“ sein. Schließlich dürfen auch bei gezielten Tötungen keine verbotenen Waffen eingesetzt werden.

1245) Artikel 51 Absatz 5, lit. b) des Protokolls I.

1246) Dazu mehr unten (2); vgl. zu den Anforderungen insgesamt: *Philipp Stroh* (2016): Humanitär-völkerrechtliche Rahmenbedingungen für den Einsatz luftgestützter unbemannter militärischer Kampfsysteme im bewafffneten Konflikt, Deutsche Stiftung Friedensforschung, Forschung DSF No. 40 (im Internet abrufbar).

1247) Für eine erhellende Kritik, *siehe Gunneflo, M.* (2016): Targeted Killing: A Legal and Political History (Cambridge University Press, Cambridge); dazu auch *Samour, N.*, Gunneflo Book Symposium (3) – Targeted Killing, Revisiting Hobbes: No Protection, No Obedience”, *Völkerrechtsblog*, 22/3/2017, https://voelkerrechtsblog.org/gunneflo-book-symposium-part-3/

1248) Vgl. Antrag der Fraktion DIE LINKE., Bundestagsdrucksache 17/12437 und Antrag der Fraktion „Bündnis 90/DIE GRÜNEN“, Bundestagsdrucksache 17/13235, Ziff. 2.

1249) Artikel 1 Absatz 1 Protokoll II.

1250) Artikel 51 Absatz 3 Protokoll I; Artikel 13 Absatz 3 Protokoll II.

1251) Artikel 51 Absatz 5 lit. b Protokoll I.

Daneben könnte bei einem Drohnenangriff eine Verletzung des Verbots der Tötung kampfunfähiger Gegner (*hors de combat*-Regel)[1252] vorliegen, weil durch den Überraschungsmoment eines Drohneneinsatzes selbst in entlegenen Regionen die Möglichkeit eines Sich-Ergebens praktisch nicht mehr gegeben ist. Selbst wenn die Betroffenen eine solche Absicht haben und dies nach dem gegenwärtigen Stand der Technik auch festgestellt werden könnte, wird ihnen für eine entsprechende Signalgebung keine Gelegenheit gegeben.

Völkerrechtlich lässt sich daraus der Schluss ziehen, dass eine Pflicht zur Verwendung milderer Mittel besteht und eine Gefangennahme einer Tötung vorzuziehen ist. Grundlage für diese Position ist eine weite Auslegung des Verbots „unnötigen Leidens" im Lichte der Prinzipien der Menschlichkeit und militärischen Notwendigkeit. Dies fordert jedoch ein fortschrittliches Verständnis der Rechtsfigur der Vermeidung unnötigen Leidens. Danach sollen Tötungen nur dann erlaubt sein, wenn sie zur Außergefechtssetzung des Gegners notwendig sind. Die Notwendigkeit ist folglich mit einer Einzelfallprüfung zu ermitteln. Zur Gewährleistung eines maximalen Schutzes des Einzelnen hat das militärische Ermessen zurückzutreten.[1253] Eine Pflicht zur Gefangennahme besteht jedoch auch nach dieser Auffassung nur dort, wo eine territoriale Kontrolle gegeben ist und die eigenen Kämpfer ausreichende Sicherheit haben, also unter strengen Voraussetzungen.[1254] Außerdem wird die *hors de combat*-Regel herangezogen, wonach Personen, die sich außer Gefecht befinden, zu schützen sind, um die Tötung verteidigungsloser oder klar unterlegender Gegner_innen zu verbieten und den Schutz des/der Einzelnen in bewaffneten Konflikten zu optimieren.[1255] Diese Regel gilt für staatliche Streitkräfte auch dann, wenn sie nicht unmittelbar an Feindseligkeiten teilnehmen.

1252) Artikel 41 Abs. 2 lit. B Protokoll I.

1253) So *Seiring, O.*, Drohneneinsätze gegen feindliche Kämpfer – Besteht eine Pflicht zur Gefangennahme als milderes Mittel?, in Frau, R. (Hg.) (2014): Drohnen (Mohr Siebeck, Tübingen), S. 100.

1254) Ausführlich dazu *Seiring, O.*, Drohneneinsätze gegen feindliche Kämpfer – Besteht eine Pflicht zur Gefangennahme als milderes Mittel?, in Frau, R. (Hg.) (2014): Drohnen (Mohr Siebeck, Tübingen), S. 83 ff.

1255) *Goodman, R.*, The Power to Kill or Capture Enemy Combatants, in European Journal of International Law (2013), Vol. 24 Nr. 3, 819-853, doi:10.1093/ejil/cht048.

Schließlich wird grundsätzlich zu äußerster Vorsicht gegenüber autonomen oder gar automatisierten Drohnen geäußert, da diese nach dem gegenwärtigen Stand von Wissenschaft und Technik, insbesondere im Hinblick auf die in den USA geführten Diskussionen über die Einführung von automatisierten Waffensysteme, nicht mehr ohne weiteres der menschlichen Kontrolle unterworfen sein werden. In vielen Fällen wird das Zielerfassungssystem viel schneller als die menschliche Wahrnehmung und diese zu langsam sein, um automatisierte Tötungsvorgänge noch rechtzeitig zu stoppen und Zivilschäden zu verhindern.[1256] Dahinter steht auch die Forderung, dass eine Entscheidung über Tod und Leben nicht von einer künstlichen Intelligenz getroffen werden und daher auch nicht auf autonome oder automatisierte Waffensysteme übertragen werden dürfe.

(2) Der Unterscheidungsgrundsatz: Nur militärische Ziele sind zulässig

Das humanitäre Völkerrecht enthält das Verbot, unterschiedslose Angriffe zu führen. Damit ist gemeint, dass bei einem Angriff jederzeit zwischen militärischen Zielen und nicht-militärischen Zielen unterschieden werden muss.[1257] Dieser Grundsatz ist eine anerkannte völkergewohnheitsrechtliche Norm und somit auch für die USA verbindlich, obwohl sie das Protokoll I selbst nicht unterschrieben hat.

Nach Artikel 48 Protokoll I sind die am Konflikt beteiligten Parteien zur Gewährleistung der Schonung und des Schutzes der Zivilbevölkerung und ziviler Objekte verpflichtet, jederzeit zwischen der Zivilbevölkerung und Kombattanten sowie zwischen zivilen Objekten und militärischen Zielen zu unterscheiden. Die Konfliktparteien dürfen ihre Kriegshandlungen nur gegen militärische Ziele richten. Als militärisches Ziel werden auch Zivilisten betrachtet, die sich unmittelbar an feindseligen Kampfhandlungen beteiligen. Gewalthandlungen sind feindselig, wenn sie in Verbindung mit einem bewaffneten Konflikt stehen, und gelten als unmittelbar, wenn die darin involvierten Personen

---

1256) Zur Problematik und Nuance der autonomen und automatisierten Drohne, siehe *Mahn-Gauseweg, C.*, Automated Warfare – Operationen unbemannter Systeme. Eine technische Systematisierung, in Frau, R. (Hg.) (2014): Drohnen (Mohr Siebeck, Tübingen), S. 1-18; *Arendt, R.* Der Einsatz autonomer Waffensysteme im Lichte des Verhältnismäßigkeits- und des Unterscheidungsgrundsatzes, in Frau, R. (Hg.) (2014): Drohnen (Mohr Siebeck, Tübingen), S. 19-34.

1257) Artikel 48, Artikel 51 Absatz 2 und Artikel 52 Absatz 2 Protokoll I.

„einen Bezug zu den Feindseligkeiten einerseits und dem eingetretenen Schaden andererseits“[1258] aufweisen.[1259]

Was als militärisches Ziel bzw. Objekt gilt, ist in Art. 52 Abs. 2 Protokoll I geregelt:

> „Soweit es sich um Objekte handelt, gelten als militärische Ziele nur solche Objekte, die auf Grund ihrer Beschaffenheit, ihres Standorts, ihrer Zweckbestimmung oder ihrer Verwendung wirksam zu militärischen Handlungen beitragen und deren gänzliche oder teilweise Zerstörung, deren Inbesitznahme oder Neutralisierung unter den in dem betreffenden Zeitpunkt gegebenen Umständen einen eindeutigen militärischen Vorteil darstellt.“

Ziel dieser Vorschrift ist es, einen möglichst umfassenden Schutz ziviler Objekte zu gewährleisten. Nicht nur müssen die Objekte als Ziel eines militärischen Einsatzes geeignet sein. Ihre Zerstörung, Inbesitznahme oder Neutralisierung muss jedenfalls prognostisch – auch noch im Zeitpunkt des Angriffs – einen eindeutigen militärischen Vorteil herbeiführen. Der Vorteil muss also bedeutend unmittelbar, bestimmt und konkret sein, also keineswegs nur hypothetisch oder potentiell;[1260] zudem muss der Vorteil militärischer Natur sein und nicht etwa lediglich einen politischen oder propagandistischen Vorteil versprechen.[1261] Ersichtlich wird auch, dass der Begriff des militärischen Ziels über den Begriff des militärischen Objekts hinaus geht und auch zivile oder sogenannte „*Dual-Use-Objekte*“ umfassen kann.[1262]

Im Zweifelsfall zu ist jedoch zu vermuten, dass ein in der Regel für zivile Zwecke bestimmtes Objekt, wie beispielsweise eine Kultstätte, ein Haus, eine sonstige

---

1258) *Platek, O.*, Autonome Kriegsführung und legitime militärische Ziele, in Frau, R. (Hg.) (2014): Drohnen (Mohr Siebeck, Tübingen), S. 46.

1259) *Melzer, N.* (2008): Targeted Killing under the International Law, (Oxford University Press, Oxford), S. 28.

1260) *Arendt, R.* (2016): Völkerrechtliche Probleme beim Einsatz autonomer Waffensysteme (BWV, Berlin), S. 64.

1261) *Platek, O.,* Autonome Kriegsführung und legitime militärische Ziele, in Frau, R. (Hg.) (2014): Drohnen (Mohr Siebeck, Tübingen), S. 47, Fn. 63.

1262) *Arendt, R.*, Der Einsatz autonomer Waffensysteme im Lichte des Verhältnismäßigkeits- und des Unterscheidungsgrundsatzes, in Frau, R. (Hg.) (2014): Drohnen (Mohr Siebeck, Tübingen), S. 23.

Wohnstätte oder eine Schule, nicht dazu verwendet wird, wirksam militärische Handlungen herbeizuführen.[1263]

(a) „Organisierte bewaffnete Gruppe“

Neben dem Status von Kombattanten und von Personen, die unmittelbar an Feindseligkeiten teilnehmen, kommen nur sog. „organisierte bewaffnete Gruppen“ als legitime Ziele von Angriffen in Betracht. Der Begriff der „organisierten bewaffneten Gruppe“ ist in Artikel 1 Zusatzprotokoll (1977) und Artikel 8 Absatz 2 lit. f des Statuts des Internationalen Strafgerichtshofs (IStGH-Statut) enthalten. Mit der Frage, inwiefern organisierte bewaffnete Gruppen als legitimes militärisches Ziel zu gelten haben, ist auch die Frage nach der Reichweite von Kriegsverbrechen gemäß Art. 8 IStGH-Statut (bzw. § 8 Völkerstrafgesetzbuch) verbunden.

Die gezielte Tötung des deutschen Staatsangehörigen *Bünjamin Erdogan* am 4. Oktober 2010 in Mir Ali in Pakistan durch eine Kampfdrohne hat auch die deutschen Strafverfolgungsbehörden mit der Frage beschäftigt, ob Bünjamin Erdogan als legitimes Ziel, also als Mitglied einer „organisierten bewaffneten Gruppe“ gesehen werden kann. Der Generalbundesanwalt kam zu dem Ergebnis, dass die Tötung von *Bünjamin Erdogan* kein Kriegsverbrechen (§§ 8 ff. VStGB) dargestellt habe und auch sonst nicht strafbar sei. *Bünjamin Erdogan* sei bei seiner Vorbereitung „auf ein Selbstmordattentat auf eine militärische Einrichtung“ im Rahmen einer gezielten Bekämpfung aufständischer Gruppierungen ums Leben gekommen. Dabei hätte sich der Drohnenangriff nicht „gegen die Zivilbevölkerung als solche oder gegen einzelne Zivilpersonen gerichtet“ und das Prinzip der militärischen Notwendigkeit erfüllt. Das verwundert, befand er sich zum Zeitpunkt des Raketeneinschlags doch in einem Haus und war eine Differenzierung zwischen Kombattanten und Zivilpersonen kaum möglich. Doch offenbar genügte der *Generalbundesanwaltschaft* schon eine bloße Kontaktschuld:

1263) Artikel 52 Abs. 3 Protokoll I.

> „Bei dem Getöteten handelte es sich nicht um einen Zivilisten, denn er gehörte einer organisierten bewaffneten Gruppe an, die Terroranschläge verübt; ohne Bedeutung ist, dass er zum Zeitpunkt des Angriffs nicht unmittelbar an Feindseligkeiten teilnahm.“[1264]

Bei seiner Anhörung im Ausschuss räumte Ministerialdirektor *Michael Koch* jedoch ein, dass es keine verbindliche Definition des bewaffneten Konflikts gebe:

> „Jeder Rechtsanwender stellt das selber für sich fest.“[1265]

Angesichts der Tatsache, dass die Hälfte der weltweit an Kriegen beteiligten Personen Mitglieder nichtstaatlicher bewaffneter Gruppen sind, vermag dieser ins Ermessen des Rechts- oder gar Waffenanwenders gestellte Feststellung über das Vorliegen und die Zugehörigkeit einer Person zu einer „bewaffneten Gruppe“ nicht zu genügen. Vielmehr bedarf es einer intensiven Auseinandersetzung über die jeweiligen Voraussetzungen und damit auch einer Auseinandersetzung mit dem Begriff des (transnationalen) „Terrorismus“.

Weil Mitglieder einer organisierten bewaffneten Gruppe grundsätzlich den Zivilpersonen zukommenden Schutz verlieren und somit legitimes militärisches Ziel von Kampfdrohnen werden können, ist – ebenso wie bei einer vorschnellen und pauschalen Anwendung der Regelungen des humanitären Völkerrechts im Bereich der Terrorismusbekämpfung – auch im Hinblick auf die Unterscheidungskriterien über das Vorliegen einer organisierten bewaffneten Gruppe eine restriktive Auslegung geboten. Einzelne terroristische Aktivitäten eröffnen noch lange nicht den Anwendungsbereich des humanitären Völkerrechts.[1266] Die Gewaltanwendung muss nach Artikel 1 Protokoll II lang anhaltend und koordiniert sein und eine gewisse Intensität erreicht haben; zudem muss die bewaffnete Gruppe einen gewissen Organisationsgrad aufweisen.

1264) Generalbundesanwalt beim Bundesgerichtshof, Verfügung vom 20.6.2013, Az. 3 BJs 7/12 – 4, zitiert nach juris; Leitsatz und Gründe in NStZ 2013, S. 644-647.

1265) *Michael Koch*, Protokoll-Nr. 80 I, S. 50

1266) Internationaler Gerichtshof für das ehemalige Jugoslawien, *Tadić,* Urt. v. 7.5.1997, Nr. IT-94-1-T, Rn. 562.

Dieser ist erst dann gegeben, wenn die Gruppe unter einer verantwortlichen Führung mit einer zentral agierenden Befehlsorganisation sowie hierarchischen Kommandostruktur steht und über eigene Disziplinarregeln zur Einhaltung humanitären Völkerrechts verfügt.[1267] Dazu gehört auch die Möglichkeit der Planung und Durchführung von anhaltenden und konzentrierten militärischen Operationen durch eine *de facto*-Autorität.[1268] Zudem ist zu prüfen, ob die bewaffnete Gruppe über einen Teil des staatlichen Territoriums Gebietskontrolle ausübt.[1269]

Angesichts asymmetrischer Konfliktlagen und dynamischer Konfliktverläufe wird heute vermehrt angenommen, dass diese Voraussetzung nicht notwendig vorliegen muss,[1270] jedoch mindestens eine Indiz-Wirkung für den Organisationsgrad einer bewaffneten Gruppe hat. Mit anderen Worten: Die Gebietskontrolle gilt als wichtiges Indiz für die Fähigkeit von bewaffneten Gruppen, langanhaltende Kampfhandlungen durchführen zu können. Anschläge von als terroristisch eingestuften Gruppen, die nicht als bewaffnete Konflikte eingestuft werden können, sind somit ausschließlich nach nationalen strafrechtlichen Vorschriften zu bewerten und mit polizeilichen bzw. strafprozessualen Mitteln zu verfolgen. Notwendig ist also stets eine Einzelfallprüfung.

Nach geltender Rechtslage ist jedenfalls das unterschiedslose Zusammenführen aller möglichen, locker mit einer Kernorganisation verbundenen Personengruppen und Personen zu einer militärischen Einheit und damit deren Qualifikation als legitimes militärisches Ziel unzulässig.[1271] Personen, die eine gemeinsame Ideologie oder Feindbilder haben und vereinzelte Aktionen durchführen, sind nach strafrechtlichen Maßstäben zu verfolgen, hier greift das humanitäre Völkerrecht offensichtlich nicht.

1267) Internationaler Gerichtshof für das ehemalige Jugoslawien, Haradinaj/Balaj/brahimaj, Urt. v .3.4.2008, Nr. IT-04-84-T, Rn. 393.

1268) *Schwarz, A.*, Die Voraussetzungen einer „organisierten bewaffneten Gruppe", Frau, R. (Hg.) (2014): Drohnen (Mohr Siebeck, Tübingen), S. 270.

1269) Eingehend *Schwarz, A.*, Die Voraussetzungen einer „organisierten bewaffneten Gruppe", Frau, R. (Hg.) (2014): Drohnen (Mohr Siebeck, Tübingen), S. 271-274.

1270) Vgl. auch die fehlende Bezugnahme in Art. 8 Absatz 2 lit. f. IstGH-Statut; anders allerdings der Internationale Gerichtshof für Ruanda, Akayesu, Urt. v 2.9.1998, ICTR-96-4, Rn. 626.

1271) Vgl. auch *Städele* (2014): Völkerrechtliche Implikationen des Einsatzes bewaffneter Drohnen (Dunker & Humblot, Berlin), S. 214.

Weiter ist zu fragen, ob schon die Mitgliedschaft in einer organisierten bewaffnete Gruppe genügen kann, um eine Person mit einer Kampfdrohne gezielt töten zu dürfen. Führt mit anderen Worten bereits die Zugehörigkeit zu einer bewaffneten Gruppe zum Verlust des Zivilschutzes und macht die Betroffenen dadurch dauerhaft zu legitimen Zielen von Angriffen? Nicht zu verwechseln ist dieser Sachverhalt mit Zivilisten, die „unmittelbar an Feindseligkeiten teilnehmen" und dadurch gemäß Artikel 13 Absatz 3 Protokoll II ihren Schutzstatus verlieren.

Eine Orientierung diesbezüglich bieten die Interpretationsrichtlinien des *Internationalen Roten Kreuzes*, die einen strengeren Maßstab anlegt. Nur diejenige Mitglieder der organisierten bewaffneten Gruppen, die eine fortdauernde Kampffunktion (*continious combat function*) innerhalb der Gruppe ausüben, können legitimes militärisches Ziel sein.[1272] Besteht also eine solche fortdauernde Kampffunktion nicht, genießt die Person völkerrechtlich gesehen den gleichen Schutz wie jede andere Zivilperson auch, es sei denn sie nimmt unmittelbar an Feindseligkeiten teil, dann bleibt sie zwar Zivilist, verliert aber ihre Immunität für die Dauer der Kampfhandlungen.

Daher ist die Ansicht der *Bundesregierung*, wonach gezielte Tötungen von Kämpfern in nicht-internationalen bewaffneten Konflikten auch außerhalb von Feindseligkeiten grundsätzlich rechtmäßig seien, nicht haltbar. Eine solche Rechtsauslegung öffnet Tür und Tor für menschenrechtswidrige außergerichtliche Tötungen.

(b) Verhältnismäßigkeit bei zivilen „Kollateralschäden"?

Mit dem Status von Zivilisten nicht direkt zusammenhängend, aber für nicht-internationale bewaffnete Konflikte sehr relevant, sind die sogenannten Begleit- oder Kollateralschäden. Nach Artikel 51 Absatz 5 lit. b Protokoll I sind Angriffe, bei denen mit Toten oder Verletzungen in der Zivilbevölkerung oder der Beschädigung ziviler Objekte zu rechnen ist, verboten, wenn sie in keinem Verhältnis zum erwarteten konkreten und unmittelbaren militärischen Vorteil stehen. Dementsprechend sind Angriffe völkerrechtswidrig, wenn dabei exzessive Schäden an Zivilpersonen und zivilen Objekten

1272) Interpretive Guidance on the Notion of Direct Participation in Hostilities under International Humanitarian Law, verabschiedet von der Vollversammlung des IKRK am 26. Februar 2009, 872 International Review of the Red Cross 991, S. 1013 ff.

entstehen.[1273] Dabei darf die Verhältnismäßigkeitsprüfung nicht allgemein und schematisch bleiben, sondern muss sehr konkret und im Einzelfall erfolgen.

Vor dem Hintergrund der erwiesenen hohen Fehlerraten, Angriffe auf Ziele, die keinen Bezug zu militärischen Auseinandersetzungen aufweisen und vor allem im Hinblick auf die sehr konkrete Gefährdung aller Menschen in der Nähe von Zielobjekten, ist die Verhältnismäßigkeit von Drohnenangriffen ernsthaft zu bezweifeln.

(c) Präzisere Kriegsführung?

Im Kontext des Drohnenkriegs wird regelmäßig behauptet, dass der Einsatz von Kampfdrohnen mit einer sicheren Kriegsführung einhergeht. Tatsächlich aber führen Drohnen auch zu einer höheren

> „Angriffsfläche für informationelle Störungen und können unter Umständen durch ein Übermaß an von ihnen generierten Daten sogar zu einer insgesamt schlechteren Informationslage führen.“[1274]

Hinzu kommt, dass bei automatisierten Kampfdrohnensystemen kein Raum für menschliche Wertungsentscheidungen mehr besteht. Wertgebundene Entscheidungen über Leben und Tod werden durch Algorithmen erzeugte Trefferwahrscheinlichkeiten ersetzt. Nicht zuletzt im Hinblick auf und wegen der zusätzlichen Fehlerhaftigkeit der Kampfdrohnen erscheint es höchst fraglich, ob eine solche Kriegsführung überhaupt mit Artikel 6 IPbpR und Artikel 6 EMRK vereinbar ist. Zudem ist hier auf die Folgeverpflichtung zur Aufklärung von Todesfällen hinzuweisen.[1275]

Im Kontext des Drohnenkriegs sind vor allem die sogenannten „*signature strikes*“ besorgniserregend. Bei derartigen Angriffen werden Personen gezielt getötet, deren Identität nicht bekannt ist, die jedoch ein Verhaltensmuster an den Tag legen, das mit einem bestimmten Profil assoziiert wird.

1273) *Platek, O.*, Autonome Kriegsführung und legitime militärische Ziele, in Frau, R. (Hg.) (2014): Drohnen (Mohr Siebeck, Tübingen), S. 47.

1274) *Stroh, P.* Das Menschenrecht auf Leben im „entmenschlichten“ bewaffneten Konflikt, in Frau, R. (Hg.) (2014): Drohnen (Mohr Siebeck, Tübingen), S. 162.

1275) So *Stroh, P.* Das Menschenrecht auf Leben im „entmenschlichten“ bewaffneten Konflikt, in Frau, R. (Hg.) (2014): Drohnen (Mohr Siebeck, Tübingen), S. 162.

cc) Menschenrechtliche Bewertung

Ein Aspekt, der im Mehrheitsbericht nicht angemessen berücksichtigt wird, ist die ganz herrschende Meinung, dass auch in bewaffneten Konflikten die internationalen Menschenrechtspakte ihre Geltung nicht verlieren. Wenngleich das humanitäre Völkerrecht die maßgeblichen rechtlichen Rahmenbedingungen vorschreibt, sind die allgemeinen völkerrechtlichen Menschenrechtsgarantien als Auslegungshilfe heranzuziehen, um den menschenrechtlichen Schutz lückenlos zu gewährleisten.[1276]

Hier erlangt bzgl. der tödlichen US-Drohnenangriffe das Recht auf Leben in Artikel 6 IPbpR[1277] eine zentrale Bedeutung. Im Hinblick auf eine mögliche Unterstützung durch die Bundesregierung ist auch das in Artikel 2 EMRK[1278] verbürgte Recht auf Leben einschlägig.[1279] Wenngleich die Menschenwürde im IPbpR und in der EMRK keine eigenständige Bedeutung entfaltet, wird sie im Verbot willkürlicher Tötungen im Sinne des Rechts auf Leben widergespiegelt und dementsprechend auch in der Rechtsprechung herangezogen.[1280] Die Wirkung des IPbpR beschränkt sich nicht auf das Staatsgebiet einer Vertragspartei. Insofern effektive Kontrolle durch einen Hoheitsträger im Ausland vorliegt, greift der Schutz des IPbpR.[1281]

1276) Dazu ausführlich *Neubert, C.-W.* (2016): Der Einsatz tödlicher Waffengewalt durch die deutsche auswärtige Gewalt (Max-Planck-Institut für ausländisches und internationales Strafrecht), Berlin, Duncker & Humblot, S. 94 ff.

1277) Artikel 6 Absatz 1 IPbpR: Jeder Mensch hat ein angeborenes Recht auf Leben. Dieses Recht ist gesetzlich zu schützen. Niemand darf willkürlich seines Lebens beraubt werden.

1278) Artikel 2 EMRK (Recht auf Leben): (1) Das Recht jedes Menschen auf Leben wird gesetzlich geschützt. Niemand darf absichtlich getötet werden, außer durch Vollstreckung eines Todesurteils, das ein Gericht wegen eines Verbrechens verhängt hat, für das die Todesstrafe gesetzlich vorgesehen ist.

(2) Eine Tötung wird nicht als Verletzung dieses Artikels betrachtet, wenn sie durch eine Gewaltanwendung verursacht wird, die unbedingt erforderlich ist, um

a) jemanden gegen rechtswidrige Gewalt zu verteidigen;

b) jemanden rechtmäßig festzunehmen oder jemanden, dem die Freiheit rechtmäßig entzogen ist, an der Flucht zu hindern;

c) einen Aufruhr oder Aufstand rechtmäßig niederzuschlagen.

1279) Angesichts von EU-Einsätzen – zum Beispiel der außen- und sicherheitspolitischen Maßnahme „Operation Atalanta“ – dürfte künftig auch Artikel 2 der Grundrechtecharta der Europäischen Union mehr und mehr relevant werden.

1280) Dazu *Neubert, C.-W.* (2016): Der Einsatz tödlicher Waffengewalt durch die deutsche auswärtige Gewalt (Max-Planck-Institut für ausländisches und internationales Strafrecht) (Duncker & Humblot, Berlin) S. 82.

1281) UNHRC, Allgemeiner Kommentar, Nr. 31, 2004, Rn. 10; dazu auch *Movassat, N.* (2016): US-Drohneneinsatz von deutschem Boden aus: Völkerrechtliche und verfassungsrechtliche Probleme (Books on Demand), insbes. S. 81 ff.

Nach ständiger Rechtsprechung[1282] des Europäischen Gerichtshofs für Menschenrechte wirkt auch die EMRK extraterritorial (vgl. auch Artikel 1 EMRK). Dies ist der Fall, wenn entweder effektive Kontrolle über ein fremdes Gebiet bzw. Autorität und Aufsicht über Personen in einem ausländischen Gebiet vorliegt oder effektive physische Macht und Kontrolle über eine Person ausgeübt wird.

Berücksichtigt man, dass zahlreiche gezielte Tötungen durch Kampfdrohnen nicht in bewaffneten Konflikten stattfinden, wird die Relevanz erheblich strengerer menschenrechtlicher Vorgaben sehr deutlich.[1283] Hier ist auch darauf hinzuweisen, dass minimale Menschlichkeitsstandards unter allen Umständen zu beachten sind, auch wenn die Schwelle eines nicht-internationalen bewaffneten Konflikts nicht erreicht wird und – weil ein Ausnahmezustand geltend gemacht wird (vgl. Artikel 15 Absatz 2 EMRK) – die völkerrechtlichen Menschenrechtsgarantien bis auf einen nicht abdingbaren Kern suspendiert werden können (vgl. Artikel 4 Absatz 2 IPbpR). Im Bereich von bewaffneten Konflikten rechtfertigt Artikel 15 Absatz 2 EMRK Einschränkungen des Rechts auf Leben unter der strengen Voraussetzung, dass die Kriegshandlungen rechtmäßig sind. Rechtmäßige Gewaltakte gelten zudem nicht als willkürlich im Sinne des Artikels 6 IPbpR.

Aus diesen menschenrechtlichen Gewährleistungen folgen deutlich strengere Rechtfertigungsanforderungen für den Einsatz bewaffneter Drohnen. Das gilt vor allem für deren Verwendung außerhalb bewaffneter Konflikte. So darf die gezielte Tötung mittels einer Kampfdrohne nur durchgeführt werden, wenn für diese Handlung eine ausreichende Rechtsgrundlage in der nationalen Rechtsordnung des angreifenden Staates besteht, die zudem den menschenrechtlichen Anforderungen genügen muss. Die gezielte Tötung darf keine bestrafende Sanktion sein, sondern sie muss ausschließlich das präventive Ziel verfolgen,[1284] menschliches Leben vor rechtswidrigen Gewaltakten zu schützen (vgl. Artikel 2 Absatz 2 lit. a EMRK). Die Tötung muss absolut erforderlich

1282) Grundsätzlich EGMR, Urt. v. 23.3.1995, Nr. 15318/89, Loizidou/Türkei, Rn. 62.

1283) Grundlegend der Bericht des Sonderberichterstatters (*B. Emmerson*) über die Förderung und den Schutz der Menschenrechte und Grundfreiheiten bei der Bekämpfung des Terrorismus v. 18.9.2013, A/68/389.

1284) *Städele, J.P.* (2014): Völkerrechtliche Implikationen des Einsatzes bewaffneter Drohnen (Duncker & Humblot, Berlin), S. 320.

sein. Sie darf nicht derart vorbereitet sein, dass sie das originäre Ziel einer Operation ist, sondern ein an sich ungewolltes letztes Mittel. Vor dem Hintergrund dieser Rechtfertigungsanforderungen wird klar, dass die mittels Drohnenangriffen durchgeführten gezielten Tötungen außerhalb bewaffneter Konflikte nur in seltenen Fällen völkerrechtskonform sein können.[1285] Regelmäßig sind schon die vorbereitenden Schutzstandards für ihren verhältnismäßigen Einsatz nicht gewährleistet.

Schließlich ist auf die prozessrechtliche Verpflichtung aus Artikel 2 EMRK hinzuweisen, wonach dem verursachenden Vertragsstaat bei ungeklärten Todesfällen eine effektive behördliche Untersuchung über die Rechtmäßigkeit und die Umstände der Tötung obliegt.[1286]

Im Fall des Geiseldramas im russischen Beslan, bei dem mehr als 330 Menschen starben, hat der EGMR seine Rechtsprechung im Bereich der Bekämpfung von Terrorismus weiter konturiert.[1287] Russland wurden erhebliche Mängel beim Krisenmanagement vorgeworfen, die zu einer sehr blutigen Beendigung der Geiselnahme führten. Auch im Falle der Terrorismusbekämpfung, so der EGMR, habe der Vertragsstaat die positive Verpflichtung, Leben zu schützen und effektive Ermittlungen nach den Umständen anzustellen. Besonders neu an dieser Rechtsprechung ist die Forderung nach effektiven Maßnahmen zur Vorbeugung von terroristischen Attacken.[1288]

dd) Verfassungsrechtliche Verpflichtungen

Zum Einsatz von tödlichen Drohnen hat der Mehrheitsbericht die Ansichten der *Bundesregierung*, des *Generalbundesanwaltes* und des *Verwaltungsgerichts Köln*[1289] Raum gegeben. Dabei wurde deutlich, dass die Bundesregierung ihrer verfassungsrechtlichen Pflicht zur Unterlassung friedensstörender Handlungen sowie zum Schutz von Leib und Leben durch eine Umkehrung der Beweislage zu entfliehen versucht.

1285) *Städele, J.P.* (2014): Völkerrechtliche Implikationen des Einsatzes bewaffneter Drohnen (Duncker & Humblot, Berlin), S. 320.

1286) Grundsätzlich EGMR, Urt. 27.9.1995, Nr. 18984/91, *McCann u.a./Vereinigtes Königreich*, Rn. 161.

1287) EGMR, Urt. v. 13.4.2017, Nr. 26562/07, Tagayeva u.a./Russland.

1288) EGMR, Urt. v. 13.4.2017, Nr. 26562/07, Tagayeva u.a./Russland, Rn. 478-493.

1289) VG Köln, Urteil vom 27. Mai 2015, Az. 3 K 5625/14, MAT A NW-2/2a, Bl. 254 ff.

Nicht das Vorliegen hinreichender Anhaltspunkte für eine Vielzahl signifikant völkerrechtswidriger Drohneneinsätze könne die Kontroll- und Abwendungspflicht der Bundesregierung für den Drohneneinsatz der USA insgesamt auslösen. Vielmehr könne die an sich zu unterstellende Völkerrechtskonformität von Drohnenangriffen lediglich aufgrund einer Einzelfallprüfung bezweifelt werden. Wie der als Zeuge vernommene Leiters der Rechtsabteilung im Auswärtigen Amt, *Dr. Martin Ney*, zuständig für Fragen des Völkerrechts, hervorhob, treffe die Bundesregierung solange keine Verpflichtung, eine etwaige eigene Beteiligung, etwa durch die Zulassung der Nutzung militärischer Anlagen auf deutschem Staatsgebiet, zu überprüfen und entsprechende Ermittlungen aufzunehmen, wie ein Kampfdrohneneinsatz völkerrechtsgemäß sein könnte.[1290]

Diese Ansicht verkennt die verfassungsrechtlichen Wertentscheidungen, die insbesondere auch die Beachtung völkerrechtlicher Bestimmungen einschließt und die Bundesregierung als außenpolitische Exekutivgewalt in die Pflicht nimmt. Eine Verantwortung der Bundesregierung ist daher nicht schon dann abzulehnen, wenn Kampfdrohneneinsätze möglicherweise völkerrechtskonform sein könnten. Von Verfassungs wegen besteht eine Nachprüfungs-, Kontroll- und Ermittlungspflicht der Bundesregierung, als Bedingung einer Beteiligung – und sei es durch ermöglichendes Unterlassen eigener Handlungsoptionen – sich von der Vereinbarkeit der Einsätze mit deutschem und internationalem Recht zu überzeugen. Das gilt erst recht, soweit sich die Bundesrepublik durch die Zulassung der Nutzung militärischer Anlagen auf ihrem Staatsgebiet an völkerrechtswidrigen Kampfeinsätzen beteiligen könnte.

Die Stellungnahme der Bundesregierung macht jedoch deutlich, dass sie eine solche Verpflichtung schon nicht (an-) zu erkennen vermag, weswegen ihr Verhalten insgesamt mit dem Untermaßverbot nicht vereinbar ist. Denn im Hinblick auf die bereits gesicherten Erkenntnisse über die tödliche Wirkung von Drohnenangriffen auf Zivilisten obliegt der Bundesrepublik eine erhöhte Sorgfaltsprüfung (*due diligence*) bzgl. ihrer verfassungsrechtlichen Schutzpflichten. Insofern ist die Rechtsauslegung der Bundesregierung, wonach eine Beihilfe etwa durch die Datenübermittlung für Drohnen-

1290) *Dr. Ney*, Protokoll-Nr. 89 I, S. 38.

kriege erst beim Vorliegen einer unrechtsmäßigen Intention (*wrongful intent*) oder eines sicheren Wissens über die gezielte Tötung bzw. den Drohnenangriff anzunehmen sei, nicht vereinbar mit den strengen Sorgfaltspflichten, die bei einer realistischen Gefahr für das Leben unbeteiligter Zivilpersonen oder extralegaler Hinrichtungen obliegen.

Im Hinblick auf das Verfahren vor dem *Verwaltungsgericht Köln* hat Ministerialrat *Stefan Sohm* zum Ausdruck gebracht, dass die *Bundesregierung* zwar dem Grundrecht auf Leben und körperliche Unversehrtheit verpflichtet sei. Dies könne jedoch kein zwingender Grund sein, dem Begehren der jemenitischen Kläger nachzukommen. Die Rechtsprechung billige der Regierung einen großen Gestaltungsspielraum bei der Wahrnehmung ihrer grundrechtlichen Schutzpflicht zu, weil anderenfalls ihre außenpolitischen Handlungsmöglichkeiten unzulässig eingeschränkt würden.

Zwar ist einzuräumen, dass im außenpolitischen Bereich der Exekutive ein gewisser Entscheidungsraum zukommt, gleichzeitig ist jedoch festzuhalten, dass unbeteiligte Zivilisten nicht als „Mittel zur Rettung anderer benutzt [...] verdinglicht und zugleich entrechtlicht“[1291] werden dürfen. Dies folgt aus der Unmittelbarkeit der Unantastbarkeit der Menschenwürde, aus der im Hinblick auf das Recht auf Leben und körperliche Unversehrtheit ein Abwehranspruch gegen willkürliche Tötungshandlung und gegen diese ermöglichenden oder unterstützenden Handlungen und Unterlassungen der Bundesrepublik folgt. Im Lichte der extraterritorialen Wirkung der Grundrechte und damit auch der grundrechtlichen Schutzpflichten gilt dieses unabdingbare Schutzniveau auch im Kontext des Drohnenkriegs durch unmittelbare und mittelbare deutsche Beteiligung.

Die Faktenlage ist mit der Zurückhaltung der Bundesregierung bei der Aufklärung ihrer eigenen Rolle im internationalen Drohnenkrieg nicht vereinbar. Aufgrund von zahlreichen internationalen Berichten ist davon auszugehen, dass bei Drohnenangriffen (sehr) regelmäßig auch und ohne eigenes Verschulden Zivilisten ums Leben kommen, weshalb schon der Begriff der gezielten Tötung einen irreführenden Euphemismus

1291) BVerfGE 115, 118 – 166, https://www.bverfg.de/e/rs20060215_1bvr035705.html, Rn. 124

darstellt.[1292] Die Wahrscheinlichkeit, dass bei einem Drohnenangriff statt der anvisierten mutmaßlichen Kämpfer oder darüber hinaus sehr regelmäßig auch Zivilpersonen getötet werden, ist hinreichend signifikant.[1293]

c) Pflichten-Wahrnehmung durch die Bundesregierung

aa) Unzulänglichkeit bisheriger Maßnahmen

Die Bundesregierung hat, soweit nachvollziehbar, bislang lediglich unterschwellige diplomatische Versuche unternommen, um Kenntnis über die Aktivitäten der USA auf dem Stützpunkt Ramstein zu erlangen. Über die Versendung eines Fragebogens an die US-Regierung hinaus hat die Bundesregierung keine weiteren ersichtlichen Maßnahmen zur Erkenntnisgewinnung unternommen. Dies ist aus Sicht der Opposition angesichts der Schwere des Sachverhalts sowie des im Raume stehenden Vorwurfs der Beteiligung der Bundesregierung an gezielten Tötungen unzulänglich.

bb) Pflichtgemäße Alternativen

Im Hinblick auf die Fehleranfälligkeit von Drohnenangriffen – insbesondere im Fall der sogenannten *signature strikes* – ist in der Regel von einer Verletzung des Unterscheidungsgebots auszugehen. Bei einer hinreichenden statistischen Evidenz regelmäßiger Verletzungen des Völkerrechts wird eine exekutive Sorgfältigkeitsprüfung aktiviert, die zunächst eine effektive Aufklärungs- und Kontrollverpflichtung über die im Bundesgebiet erfolgenden Vorbereitungs- und Durchführungshandlungen im Drohnenprogramm begründet.

1292) Siehe *Neubert, Carl-Wendelin* (2016): Der Einsatz tödlicher Waffengewalt durch die deutsche auswärtige Gewalt (Max-Planck-Institut für ausländisches und internationales Strafrecht), Berlin, Duncker & Humblot, S. 117, Fn. 197; Columbia Law School (2012): Civilian Impact of Dronhes – Unexamened Costs, Unanswered Questions (Law Clinic Report); Stanford Law School/NYU School of Law (2012): Living under Drones – Death, Injury, and Trauma to Civilians From US Drone Practices in Pakistan (International Human Rights and Conflict Resolution Clinic/Global Justice Clinic).

1293) So zeigt zum Beispiel der Angriff vom 26. Januar 2015 in Hareeb in der Provinz Shabwa. Bei diesem CIA-Angriff kamen drei Personen um, von denen höchstwahrscheinlich alle Unbeteiligte waren, darunter auch ein Kind, dazu The Guardian: http://www.theguardian.com/world/2015/feb/10/drones-dream-yemeni-teenager-mohammed-tuaiman-death-cia-strike .

Weiterhin müssen die jeweiligen Fachaufsichten der Bundesministerien und des *Bundeskanzleramtes* ihre Genehmigungs- und Anordnungspraxis betreffs der Übermittlung personenbeziehbarer Daten an ausländische Stellen auf eine denkbare Anschlussverwertung für die Vorbereitung gezielter Tötungen hin überprüfen und durch effektive Maßnahmen sicherstellen, dass diese nach bestem Wissen und Gewissen ausgeschlossen werden kann.

Damit korrespondiert aus dem Gewaltenteilungsprinzip ein umfassender Informationsanspruch der zuständigen parlamentarischen Gremien des Bundestages bzw. eine Informationspflicht der Bundesregierung sowohl über die von ihr ergriffenen Maßnahmen als auch über den Stand ihrer Kenntnisse. Schließlich hat die *Bundesregierung* gegenüber den *NATO*-Verbündeten dafür Sorge zu tragen, dass die Bundesrepublik außerhalb ihrer Bündnispflichten nicht an völkerrechtswidrigen Agressionsakten mitwirkt. Dabei kommt ihr zwar ein großer Gestaltungsspielraum zu, dieser darf im Rahmen einer Gesamtabwägung der außen- und innenpolitischen Interessen sowie dem Interesse der Bundesregierung an einer funktionsgerechten und organadäquaten Aufgabenwahrnehmung jedoch nicht dazu führen, dass sie sich jeglicher Maßnahmen zum Schutz des Lebens enthält oder Einrichtungen zur Durchführung extralegaler Hinrichtungen in ihrem Verantwortungsbereich vorzuhalten. Vielmehr müssen Kenntnis oder Anhaltspunkte für eine Beteiligung deutscher Stellen am US-Drohnenprogramm konsequent überprüft und abgestellt sowie die Gestattung der Überlassung und Nutzung von Militäreinrichtungen auf deutschem Hoheitsgebiet an das Völkerrecht gebunden werden.

Insbesondere müssen die verfassungsrechtlichen Bestimmungen des Grundgesetzes nicht hinter den Bedürfnissen und Anforderungen der in Deutschland stationierten ausländischen Streitkräfte zurücktreten. Vielmehr sind auch diese im Rahmen ihrer Tätigkeiten im Bundesgebiet den grundlegenden Regelungen unterworfen[1294]. Weder dürfen die US-Truppen in Ramstein einen Angriffskrieg vorbereiten oder starten noch darf

1294) Vgl. Art. II des NATO-Truppenstatuts von 1951.

die Bundesregierung dies zulassen oder unterstützen. Ebenso wenig darf von deutschem Boden eine „Friedensstörung“ im Sinne des Art. 26 GG ausgehen oder von hier aus Unterstützung erfahren.[1295]

In diesem Sinne können die Handlungen der Exekutive auch zum Gegenstand einer strengen gerichtlichen Kontrollbefugnis gemacht werden. Die Gerichte müssen zwar die originäre Zuständigkeit der Bundesregierung für die Gestaltung der außenpolitischen Beziehungen und den sich daraus ergebenden Gestaltungsspielraum der Exekutive wahren, anders als im Falle der weiten Einschätzungsprärogative der Legislative geht die gerichtliche Überprüfung von Handlungen der Exekutive über eine bloße Evidenzkontrolle hinaus. Sie verpflichtet die Gerichte zur Kontrolle der von der Exekutive unternommenen Maßnahmen im Hinblick auf eine sorgfältige Tatsachenermittlung und die Bildung angemessener Abwägungsvoraussetzungen für die Ergreifung effektiver Maßnahmen zur Sicherstellung menschenrechtlicher Mindeststandards. Kommt die Exekutive ihrer Ermittlungspflicht nicht nach oder geht sie trotz valider Indizien für Völkerrechtsbrüche im Einzelfall davon aus, dass die übrigen Einsätze mit dem Völkerrecht vereinbar sein werden, so hat das erkennende Gericht eine Verletzung des Untermaßverbots festzustellen.

In einem zweiten Schritt stellt sich die Frage, ob die Aktivierung einer Sorgfältigkeitspflicht nicht auch mit einer Umkehrung der Beweispflicht einhergeht, wonach es der Bundesregierung obliegt, zu beweisen, dass eine etwaigen Beteiligung Deutschlands an völkerrechtswidrige Drohnenangriffe auszuschließen ist. Anderenfalls droht eine Aushöhlung der gerichtlichen Überprüfung von Akten der Kriegsführung, die schließlich in eine menschenrechtswidrige Rechtlosstellung in bewaffneten Konflikten münden würde.

1295) *Dieter Deiseroth* (2009): Das Friedensgebot des Grundgesetzes und der UN-Charta, Betrifft Justiz Nr. 99,S. 143-149.